COSMOS
Navigate the Compliance Universe

CEP Magazine - September 2020
If you can't protect data, don't collect data

By Dean Gonsowski, JD, BS

Dean Gonsowski (dean.gonsowski@activenavigation.com) is the Chief Revenue Officer for Active Navigation, which is headquartered in the Washington, DC, metro area.

- twitter.com/dean_gonsowski
- linkedin.com/in/dean-gonsowski-2a469/

"There are only two types of companies: those that have been breached and those that don't know they have." - Elena Kvochko and Rajiv Pant, *Harvard Business Review*.[1]

In 2019 in the US, there were 1,473 data breaches and more than 160 million records exposed.[2] This relentless attack on consumers' personal data has led to several global data privacy regulations being enacted—notably the California Consumer Privacy Act (CCPA) in the US and the European Union's General Data Protection Regulation (GDPR). With so many new state-specific laws also being passed at a rapid pace, it is getting harder for compliance professionals to meet all the requirements of these complex laws—many of which are still in flux. With the compelling need for data protection, what does this mean for compliance officers?

The challenges of competing data protection laws

Different statues and regulations apply depending on the type of data you are handling, rather than the specific enterprise or industry. For example, in the US, health and patient data are subject to the Health Insurance Portability and Accountability Act. Financial information is subject to myriad regulations under the Securities and Exchange Commission, including the Sarbanes-Oxley Act and the Federal Information Security Management Act.

Different geographies also mandate different protection. For example, while all 50 states have now passed security breach notification laws, each state has different definitions of what constitutes "data" and "breach."[3]

Certain industries can also have "pseudo-laws" like the recently released National Institute of Standards and Technology Privacy Framework, which is a voluntary tool built to help public and private sector entities "identify and manage privacy risk to build innovative products and services while protecting individuals' privacy."[4]

With so many competing, complementary, and sometimes conflicting regulations, it can be an arduous undertaking for compliance professionals to navigate the intricacies of these regulations. To complicate matters further, as privacy laws become more expansive, the penalties for noncompliance are becoming riskier—not to mention costlier. This means that compliance with burgeoning data protection laws is more important than ever.