COSMOS
Navigate the Compliance Universe

CEP Magazine - November 2019
Continuous monitoring is required for effective data privacy and security

By Ambler T. Jackson

Ambler T. Jackson, CIPT, CIPM, CIPP US/G, JD, is a privacy subject matter expert located in Washington, DC, USA.

- linkedin.com/in/amblertjackson/

Continuous monitoring is the maintaining of ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions.[1] One US federal government resource describes continuous monitoring as a risk management approach to cybersecurity that maintains an accurate picture of an agency's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies.[2] In the financial industry, continuous monitoring has been described as an "automated, ongoing process that enables management to assess the effectiveness of controls and detect associated risk issues; improve business processes and activities while adhering to ethical and compliance standards; execute more timely quantitative and qualitative risk-related decisions; and increase the cost-effectiveness of controls and monitoring through IT solutions."[3]

Recent events related to personal data and security have given rise to the increasing need to continuously monitor business processes and the entire data life cycle. As such, it is a best practice—and in the case of federal agencies, it is a long-standing practice—to develop and adhere to a continuous monitoring strategy. Continuous monitoring involves an ongoing process that requires management to continuously review business processes in order to appropriately mitigate risk associated with collecting, maintaining, and using personal data. Most professionals in a management function or role, or who have management responsibilities, understand that continuous monitoring is an important risk management tool; however, many professionals in management are just now beginning to understand why continuous monitoring is critical and absolutely necessary for business operations across the enterprise.

Continuous monitoring is typically discussed as part of a framework for managing risks. There are several kinds of risks (e.g., strategic, operational, financial, compliance). Within the operational and compliance risk areas, from a data privacy and security perspective, new risks are emerging daily. Without enterprise-wide continuous monitoring, it will be nearly impossible to proactively identify and mitigate new risks. Enterprise-wide risk management allows an entire organization to contribute to mitigating risk; this includes everyone from the frontline employees, technical experts, and management to executive leadership. The approach takes into consideration the mission, objectives, business functions, and processes of the organization as well as the culture and appetite for risk.

What is personal data?

Fundamentally, your personal data is data that identifies you. For example, if I ask you to provide me with your personal information so that I can contact you and ask that you provide feedback on the topic of this article, you may provide me with your email address and phone number. These two data elements are personal to you. No two

people share the same email address or telephone number. Upon reading the request, you will immediately understand that I am referring to your data. So, on the one hand, given the context of this example, most people will agree that the term personal data is self-explanatory.

On the other hand, personal data may take on a different meaning and result in a different privacy impact depending on several factors, including, but not limited to, the purpose for which data is collected, how it is used, and by whom. There's no one global definition for personal data. The legal and regulatory definition and description of personal data may vary according to, for example, the citizenship of the individual to which the data belongs, the type of data collected, the industry to which the data pertains, and other variables.

For example, in the United States, the government describes personal data using the phrase personally identifiable information (PII), and PII is defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) and information that is linked or linkable to an individual, such as medical, education, financial, and employment information."[4]

At the state level, at least in California, personal data is expressed as personal information. According to the California Consumer Privacy Act (CCPA), personal information means information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device...."[5] Under the European Union's General Data Protection Regulation (GDPR), personal data is any information that relates to an identified or identifiable living individual.[6] The Brazilian General Data Protection Law (LGPD) defines personal data as any information related to an identified or identifiable natural person."