GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Karnas, Mathew

"How GDPR Teaches Us to Take a Bottom-Up Approach to Privacy"

Darkreading.com

URL: https://www.darkreading.com/endpoint/privacy/how-gdpr-teaches-us-to-take-a-bottom-up-approach-to-privacy-/a/d-id/1335058

Accessed: 09 July 2019

Synopsis: With the introduction of major, new regulatory rules and requirements, privacy has become an enhanced area of focus for many organizations. That focus has often focused on compliance-related activities, one regulation at a time. But when it comes to privacy, organizations often don't realize that compliance shouldn't be their sole focus — solving their underlying security and data problems should be the real goal. Approaching privacy via a top-down, checklist mentality simply to meet regulation provides a limited, perfunctory privacy stance that delivers little real security. Adjusting to a bottom-up approach — that is, shifting the focus to address underlying security needs and utilizing data management best practices — sets up organizations to achieve both regulatory compliance and a strong privacy posture.

DARKReading

6/28/2019
10:00 AM

Matthew Karnas
Commentary
Connect Directly

How GDPR Teaches Us to Take a Bottom-Up Approach to Privacy

Looking at underlying security needs means organizations are more likely to be in compliance with privacy regulations.

As we pass the one-year anniversary of the General Data Protection Regulation (GDPR) and look ahead to the upcoming enforcement of the California Consumer Privacy Act (CCPA) on January 1, 2020, what do privacy best practices look like? How should organizations approach compliance?

With the introduction of major, new regulatory rules and requirements, privacy has become an enhanced area of focus for many organizations. That focus has often focused on compliance-related activities, one regulation at a time. But when it comes to privacy, organizations often don't realize that compliance shouldn't be their sole focus — solving their underlying security and data problems should be the real goal. Approaching privacy via a top-down, checklist mentality simply to meet regulation provides a limited, perfunctory privacy stance that delivers little real security. Adjusting to a bottom-up approach — that is, shifting the focus to address underlying security needs and utilizing data management best practices — sets up organizations to achieve both regulatory compliance and a strong privacy posture.

A Bottom-Up Approach to Privacy

A bottom-up, security-driven, and data-focused approach is a better solution for meeting privacy requirements like GDPR. A bottom-up approach is tailored to an organization's specific needs. It secures and manages data based on those unique needs as well as the requirements of a regulatory body: It can incorporate compliance while still prioritizing customers and their data over checking boxes. Part of the bottom-up approach to tailoring a privacy program is to thoroughly understand threats and risks as they relate to the security and management of underlying customer data. This facilitates identification of key privacy use cases, appropriate program design adjustments, and prioritization efforts.

There are multiple elements to building an effective privacy program but the following considerations are commonly overlooked when chasing compliance: *privacy by design*, which supports bottom-up *data protection* and *process automation*.

Privacy by Design

Long before its incorporation into GDPR, the concept of privacy by design was developed by recognized privacy expert Dr. Ann Cavoukian. Privacy by design and its foundational principles involve embedding privacy into underlying processes, objectives, operations, and technologies by default. In an effort to make privacy by design more practical when designing and implementing solutions that meet GDPR requirements, a group of European privacy experts examined privacy-by-design concepts through privacy use cases, strategies, and implementation tactics. Their work provides a framework in terms that are more easily applied to data and processes and more relatable from software and engineering perspectives.

Effective privacy by design explicitly serves customers and their privacy needs. It drives both data protection (such as security engineering, including pseudonymization) and process automation (such as data subject access requests, including "delete my data") efforts.

Data Protection

Securing customer data from the bottom up requires a strong data security program as a foundation. This provides an overall direction and approach for data security and includes policies, standards, and procedures that align with the tenets of privacy by design. To implement these tactics, it is necessary to understand both the locations and types of data — you can't protect what you don't know exists. The utilization of technology should be *one* component of protecting data; it is important to use technology where necessary as part of a multifaceted of program instead of purchasing products and expecting them to deliver compliance and security singlehandedly.

Process Automation

Successful privacy programs require operationalized processes that are repeatable, auditable, and automated. As privacy demands increase from both internal and external customers, adding additional staff resources provides only limited scalability; automated processes become increasingly critical. In particular, data subject access requests are a common process to automate, but there are others that benefit from operationalization, such as:

- Data classification and mapping
- Data privacy impact assessment
- Third-party data management
- Data incident response

Even when automated, privacy-related processes should be treated as operational: They should be reviewed and maintained on a dynamic, day-to-day basis and not treated as a static, one-off set of procedures. Organizations should adopt operationalized privacy as part of their perspective and culture.

Privacy regulations such as GDPR will continue to be introduced in an effort to compel organizations to properly secure and handle customer data. But regulatory compliance alone doesn't guarantee an organization has an effective privacy program. Regulations provide top-down mandates to meet but minimal guidance on how to achieve an effective privacy program that addresses the unique needs of a specific organization. To truly advance privacy, as well as compliance, organizations must dig deep to understand the root causes of their individual privacy challenges and implement approaches with a bottom-up mentality.

Related Content:

- GDPR's First-Year Impact by the Numbers
- A Rear-View Look at GDPR: Compliance Has No Brakes
- GDPR Drives Changes, but Privacy by Design Proves Elusive

- 3 Ways Companies Mess Up GDPR Compliance the Most
- With GDPR's 'Right of Access,' Who Really Has Access?

Matthew Karnas is the Cybersecurity & Risk Practice Lead at Sila and has over 18 years of experience providing professional services to Fortune 500 companies and the Federal government across multiple verticals and agencies. Matt brings a unique mix of technical and ... View Full Bio