Developing a Data Privacy Program That Works

How Do You Implement a Privacy Program?

As information professionals, we are inundated with warnings about the consequences of contravening, however inadvertently, data privacy laws and regulations. The flurry of recent legislation, meant to protect consumers, has unintentionally resulted in chaos for global companies trying to make sense of the laws and demonstrate compliance.

While resources for understanding the letter of the law are plentiful, practical guidelines for enacting a privacy program are not. To fill that gap, here are some actionable steps for assuring data privacy. But first, let's examine several conditions that make a thoughtful and codified approach to data privacy so essential today. We'll also include some recent research on trends in privacy and information governance.

Drivers of Transformation in Data Security

Data security and compliance are on the minds C-suite leaders in all industries. It seems like every week there is yet another high-profile data security breach to which the world's most tech-savvy companies are falling victim. In 2019, 2.7 billion identity records were exposed by hackers and placed for sale on the internet.[1] Perhaps the most publicized breach involved Facebook – a hack exposed the personal information of nearly 50 million users. But Facebook is not alone. Quest Diagnostics, Houzz, and Capital One are just three of the many name-brand organizations that joined the list of high-profile hacks last year.

Data privacy is on the minds of C-suite leaders in all industries. It seems like every week there is yet another high-profile data security breach.

At the same time, data protection regulations around the world are becoming increasingly strict. One prominent example is the General Data Protection Regulation (GDPR) in Europe; another is the California Consumer Privacy Act (CCPA) – and other statutes are being implemented across the globe. There are also many guidelines that do not have the force of law, but are part of self-regulatory frameworks that are considered industry best practices.

With concern over data security intensifying, organizations are putting their money where their mouth is. According to AIIM research, 51% of organizations say that they are planning to spend "more" or "a lot more" on information governance, records management, and digital preservation over the next 18 to 24 months.[2]

Steps to Developing a Privacy Program

How can organizations increase their data privacy efforts? Here are some essential steps to consider.

1 Develop a Project Roadmap

A written project roadmap is critical to providing a manageable overview of your data privacy program. This is where you codify the scope, significant milestones, and dependencies of your project. Here are some important questions to ask:

- What specific information and data types require privacy policies?
- What personally identifiable information do we *need* to collect and use?
- What is the appropriate life cycle for personally identifiable information and sensitive data?
- What timelines and milestones must we meet for our privacy program to be successful?
- How and when will we reassess our privacy program on an ongoing basis?

2 Establish Roles and Responsibilities

Clearly defined roles and responsibilities are the backbone of a successful data privacy program. Your plan must hold people formally accountable for doing the "right" thing at the "right" time – and this requires the definition and deployment of roles that are appropriate for the culture of your organization. A few common roles include:

Chief Privacy Officer – A senior-level executive responsible for managing risks related to information privacy laws and regulations.

Data Protection Officer – An independent senior or technical-level resource who ensures that the organization applies the laws protecting the personal data of individuals.

Privacy Officer – Part of a cross-functional team responsible for building a culture of privacy, raising awareness, and ensuring compliance across the enterprise.

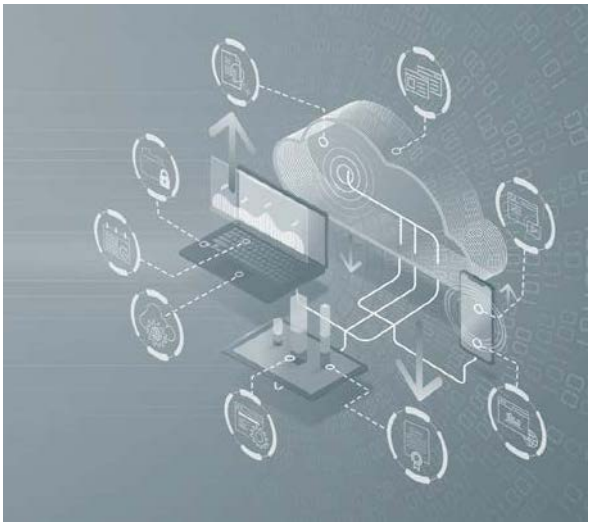
Data Owner – Individuals across the organization accountable for the data within a specific domain or process.

Data Steward – Subject matter experts and process owners with accountability for the day-to-day management of data.

3 Develop a Training Plan

Data privacy is everyone's responsibility, and everyone in the organization should be trained in the systems and processes put into place to ensure compliance.

Most privacy statutes do, in fact, require training. Under the GDPR, for example, companies are compelled by law to provide their employees with internal privacy training on data protection. You can do this through workshops, online training, and interactive exercises to make sure everyone is up to date with policies and procedures. Users should, for instance, know which types of data they are not allowed to modify or share with third parties, recognize fraudulent attempts to obtain personal information, and understand the consequences of carelessness when it comes to data privacy.



Notes:

1. Gizmodo. *Mother of all Breaches.*
2. AIIM Industry Watch. *Automating Compliance and Governance*.

Moving Forward

The burden of assuring data security and regulatory compliance demands greater levels of information governance. Data hacking is at an all-time high, regulations are getting stricter, and organizational risks have never been more demanding. Consider these steps as you design your data privacy program. Look for providers and partners with the right mix of capability, vision, and expertise to help you properly secure and protect private information.

Authored by:

Kevin Craine, MBA
Content Strategist, AIIM
Host and Producer of *AIIM On Air* Podcast

AIIM
8403 Colesville Road, Suite 1100
Silver Spring, MD 20910, USA
+1 301 587 8202
www.aiim.org

AIIM Europe
Office 1, Broomhall Business Centre,
Worcester, WR5 2NT, UK
+44 (0)1905 727 600
www.aiim.org