Using Data Privacy Technology in a Developing Regulatory Ecosystem

Article By:

Colleen M. Yushchak

As data privacy regulations have become increasingly commonplace in the last decade, organizations have had to strategically assess how they collect, process, store, and sell consumer data. To better equip themselves for this evolving landscape, many are utilizing data privacy technology to support compliance requirements. Data privacy technology allows organizations to comply with existing regulations and prepare for future regulations by offering a more streamlined, documented, and in some cases automated solution to address privacy.

Data Privacy Technology

Organizations have a variety of technology platforms to choose from, including well-known and comprehensive solutions such as OneTrust, TrustArc, WireWheel, and Securiti.ai to more niche and solution specific tools. These platforms act as a centralized interface for assessing and managing privacy, information governance, risk, and overall compliance for organizations. With a lack of a global standard for data privacy regulations, these tools allow for the automation of Data Protection Impact Assessments (DPIAs), creation of data inventories, design of compliance programs, managing of cookie banners and notices, and many other services currently required by current or emerging regulations. The advantage of using data privacy technologies is their ability to centralize information into a single platform to increase visibility into how personal information is collected and processed throughout businesses to meet regulatory compliance needs. It also can automate many privacy processes that would otherwise place a burdensome workload on internal privacy departments.

Privacy management tools can help an organization create and maintain:

Privacy Risk Assessments

Often, the first step in developing a privacy program involves performing an Enterprise Privacy Risk Assessment. In some cases, organizations don't have the time, resources, or budget to perform a formal, in-person, comprehensive assessment. In many cases, several dozen people across various functional areas (IT, HR, Marketing, Legal, Compliance, Analytics, etc.) must provide input. This is where a privacy management tool can help to make that process more streamlined, allowing key stakeholders to contribute to a risk assessment on their own time. Privacy management tools allow

organizations to obtain real-time insights and analytics in order to identify their largest privacy compliance gaps and risks in order to develop a roadmap for their privacy program.

Data Inventory

A properly maintained data inventory captures comprehensive details on the personal information that is being collected, stored, and used by an organization. When properly constructed, a data inventory should include a listing of assets that store personal information and processing activities that use personal information. Privacy management tools allow businesses to utilize automation and workflows to query internal stakeholders on how personal information is processed and stored enterprise-wide. Some privacy management tools have automated data discovery and automation technologies that can be used to build the data inventory. This limits data sprawl and better equips a business to maintain compliance with regulatory requirements as they develop. A current and comprehensive data inventory can be used to support the development of privacy notices, adjudication of data subject access requests, and operationalization of records retention requirements.

Data Protection Impact Assessments (DPIAs)

A DPIA, or Privacy Impact Assessment (PIA), is used to identify and mitigate risks associated with the processing of personal information. Privacy management tools make it much easier to incorporate these assessments into existing business processes. This is especially true if you also have your data inventory within the same privacy tool, as often high-risk processing activities are identified through the data inventory.

Data Subject Access Requests (DSARs)

Under current regulations, individuals in certain states have rights relating to the personal information collected on them by organizations. These rights include the right to request access to, a copy of, correction to, and deletion of their personal information. In addition, individuals can opt in or out of certain processing activities. Privacy management tools allow an organization to automate the adjudication of these rights requests. Privacy management tools are especially helpful in supporting the opt-in/out of certain processing activities because there is a requirement for organizations to obtain users' explicit opt in/out consent. Privacy management tools allow organizations to easily track consent in a central location to demonstrate compliance with these various rights. In addition, many of these regulations require an organization to maintain a log of all privacy rights requests, along with key information about the timing of response and outcome. Privacy management tools allow for automated tracking of requests that allows organization to comply with the record keeping requirements.

Cookie Compliance

New privacy rights that allow individuals to opt-out of the sale of data are requiring organizations to take a closer look at how they are handling cookies on their websites. In many cases, certain third-party advertising cookies are considered a sale of data, and now require the individual to be able to opt-out of that sharing/sale. Privacy management tools provide a good solution for organizations to scan, analyze and bucket their website cookies to ensure that organizations are using cookies only in ways permitted by data protection laws. Many of the tools provide pre-generated or customizable templates for branding to apply the latest changes in global laws and frameworks to a website's cookie banner.

Final Thoughts

While the previously listed capabilities do not encompass all the privacy related solutions offered through privacy management tools, they do illustrate the benefits of employing a privacy management tool to automate and centralize privacy compliance activities. Using privacy technologies in the right way can accelerate compliance with supporting documentation efforts, automate complex privacy processes, and provide a framework for organizations to create and monitor their privacy programs.

Akash Mainali also contributed to this article.

Source URL:https://natlawreview.com/article/using-data-privacy-technology-developing-regulatory-ecosystem