Adviser: Strengthen your data mapping in the era of GDPR

By STEVEN G. STRANSKY

May 26, 2018 (Crain's Cleveland Business) -

Between the time the General Data Protection Regulation (GDPR) was approved by the European Union in April 2016 and came into force in May 2018, private sector organizations across the globe have spent billions of dollars on lawyers, consultants, compliance officers and information technology enhancements to ensure that their business practices align with the regulation's requirements.

Given both the importance of data privacy and the fact that the GDPR empowers supervisory authorities to issue significant fines and penalties for certain GDPR violations, compliance with the European legal framework is not — and should not be — a one-time exercise. Yet, post-GDPR compliance does not have to be a separate endeavor, and businesses can transition a key aspect of their preparation work — data mapping — into the foundation of a broad and continuous compliance regime.

In order to determine the applicability of the GDRP, it logically follows that an organization needs to understand the scope and nature of the information it processes. Accordingly, in preparing for the GDPR, organizations may have already undertaken data mapping efforts to identify who in their organization processes personal data; the types and categories of personal data they process; the methods in which this data is collected; the external and internal parties to whom the data is disseminated; and the physical locations where the data is retained. In other words, data mapping provides an organization with a better understanding of the "who, what, when, where, why and how" of its data processing life cycle.

Consequently, pre-GDPR data mapping efforts will form the foundation for maintaining compliance with what are likely to be some of the GDPR's most

highly scrutinized requirements: privacy notifications, the invocation of data privacy rights, record-keeping, data processing agreements and data breach response.

For instance, the GDPR sets forth a broad range of requirements governing the content, scope and manner of privacy notifications. More specifically, these provisions require controllers — the people or businesses who determine the purpose and manner in which personal data is processed — to notify data subjects on, among other things, the purpose of data processing, the recipients of the personal data, and of their intent to transfer personal data to a third country or an international organization. The underlying purpose of these privacy notices is to facilitate fair and transparent data processing and ensure individuals are aware of the risks, rules and safeguards in relation to the processing. An organization should be able to rely upon its data mapping results to provide data subjects with a narrowly tailored privacy notice, which conforms with both the intention and spirit of the GDPR.

Separately, the GDPR provides data subjects with several rights related to the collection, processing and retention of their personal information, including the rights of access, rectification, erasure and restriction. The GDPR, however, provides certain exceptions and caveats with regard to these provisions. Through data mapping, an organization is better prepared to respond to data subjects who invoke their rights under the GDPR because it knows what data is in its possession, when it was collected, where it is stored and why it is being retained. Having an accurate and current data map will enable an organization to efficiently and effectively respond to requests or complaints from data subjects, which ultimately will limit any potential liability in this context.

The "records of processing activities" clause mandates that organizations demonstrate, in writing, compliance with the GDPR. More specifically, under certain circumstances, organizations are required to maintain documentation that memorializes the purposes of their data processing activities; describes the categories of personal data they process; identifies the individuals to whom personal data will be disseminated; and details international data transfers.

Moreover, the regulation provides that these organizations (or their representatives, when applicable), shall make these records available to the supervisory authority, upon request. The UK's Information Commission Office has not only endorsed data mapping as a method for maintaining compliance, but has recommended that organizations expand their data mapping efforts beyond the "who, what, when, where, why and how" framework, and incorporate into it all GDPR-compliance related issues, such as controller-processor agreements, data protection impact assessments and records concerning personal data breaches.

To demonstrate compliance with the GDPR, the controller "should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default." Accordingly, an organization's data mapping efforts should be leveraged into its day-to-day internal processes and procedures.

In other words, by maintaining an evolving and accurate map of its personal data, an organization will be building a meaningful and thorough GDPR-compliance program for the future.

Stransky is senior counsel in Thompson Hine's business litigation and privacy and cybersecurity practice groups.