Sienna Group

A Foundational Approach to Complying with GDPR

Sienna Group
9644 Linebaugh Avenue
Tampa, FL 33626

Public

(800) 792-6421
www.siennasecure.com

"Over half of US multinationals say GDPR is their top data-protection priority"

– PwC Pulse Survey, December 2016

The approved EU General Data Protection Regulation (GDPR) is a significant update to the previous regulation. It was designed to add uniformity throughout the member countries, to afford enhanced protection of personal data for residents and workers in the EU.

This update was necessary given the vast amounts of data proliferation, lack of clarity surrounding cloud services and the inability to effectively govern past interpretations of the legacy Directive. The deadline for compliance was May 2018. The penalties for non-compliance associated with data breaches is expected to be significant and could be as high as 4% of annual turnover, or €20,000,000, whichever is greater.

This represents an immediate challenge for organizations, given that the accuracy and acknowledgement of data breaches today, continues to hover around four to six months after the breach occurrence. This lack of timely reporting, highlights the importance of having requisite knowledge of the use and behavior of personal information.

Unfortunately, most organizations do not have a solid grasp on the amount of personal data that is created, shared, processed and stored, all of which will be exacerbated as the May 2018 deadline for GDPR compliance looms. While GDPR is an overarching program, there are three key areas that firms can leverage to ensure their risk of non-compliance remains low, along with ensuring advocacy in protecting the personal data of EU citizens and workforce.

Role Review

In order to successfully comply with the new regulation, a review of the roles that have been defined in the GDPR is valuable, as it serves as a mapping of the data flows and subsequent protection measures. To this end, the following roles have been defined:

- Data Subject – individual EU Citizen or person working with the EU
- Data Controller – Organization leveraging personal data for business purposes
- Data Processor – Cloud/Data storage provider
- Data Protection Officer – accountable individual required for larger organizations

Article 24 of the GDPR specifies the responsibilities of the data controller. The controller has the key role in directing the processor as to the expected and proper use of the data, as well as, coordinating with the data subjects should a breach occur.

Given the centrality of this role, it is vital the controller possess the technical and organizational measures needed to identify, classify, protect and minimize the use of personal data, along with specifying a reasonable retention period for its use. Regardless of how data is processed today, it would be beneficial for firms to view the flow of data with respect to these roles.

Privacy Impact Assessments

Article 35 of the GDPR describes Data Protection Impact Assessments

*"Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact** of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

The key point of this section, is the assessment be carried out **prior** to any processing. This is a challenge for most organizations given they do not have detailed knowledge of their unstructured data, nor how it is used in context of the role of a processor. A foundational approach to resolve this, is to properly classify personal data at rest for existing data and upon creation for new data, using a persistent approach that maintains state across infrastructures. Gateway classification that does not properly label personal data, is insufficient in determining the level of risk, nor does it apply a consistent protection mechanism.

Data Security

Article 32 of the GDPR describes technical and organizational measures that firms should take to ensure the protection of personal data.

By having a fundamental knowledge of the scope of personal data, appropriate measures can be implemented, along with retention periods for anticipated usefulness. What is also important to understand, are the trends and behaviors that occur over time in the relationship between the data subject, controller and processor, in order to prevent breaches, or have rapid acknowledgment when one occurs. For large organizations, this task will likely be addressed by the Data Protection Officer (DPO).

The DPO will need to have the technical means to report on personal data that is being accessed by the processor, including transfers to external entities outside of the EU. Given the dynamic nature of business relationships, real-time visualization of the data and behaviors allow for positive modifications to the security posture to occur. This also has a positive effect on the data protection impact assessment, regarding the likelihood of high risk to the rights and freedoms of natural persons. Without this visibility, it is unlikely that a DPO can effectively report to the Controller that the data is being created, shared, processed and stored appropriately.

Conclusion

GDPR is a broad and overarching regulation which will require a change in perspective for firms collecting personal data in support of their business. While many of the current controls convey aspects surrounding the roles that are defined, they don't dictate the flow and expectations of appropriate use.

The concepts surrounding the data protection impact assessments could prove difficult for many firms, if they do not possess the ability to identify personal data in either structured, or unstructured data stores. By discovering personal data at rest and ensuring that data is classified as it is created, more succinct knowledge of the data and the associated risks can be obtained.

The protection of data based on the classification attributes can more easily be determined and applied through access control, or encryption as an example. Along with this is the ability to define the business usefulness of the data, which can be established at creation to ensure proper disposal, as well as the ability to erase personal data upon request.

While these three concepts alone do not cover the entirety of a GDPR Program they represent foundational approaches to understanding, visualizing, and protecting personal data through the use of classification.