GDPR – What to Expect in the Coming Months

October 24, 2017

The General Data Protection Regulation (GDPR) is a new European data privacy regulation that will be fully enforced from on May 25th, 2018, after being ratified in April 2016. The time period between the two dates was designed to be the grace period for companies to use to be fully compliant by the due date.

GDPR is also designed to be a privacy regulation that has more consideration for the data subject (you and me) rather than the business. Most regulations have concepts of privacy but not with the full consideration of the data subject and can have the appearance of protecting the business as the primary purpose.

With GDPR, regardless of the location of the company, if you process GDPR data (which is defined as personal data that originates from the EU) then you would fall under the regulation and have the potential for hefty fines. Fines in the neighborhood of EU20MM or 4% of global gross revenue…whichever is greater.

There are also three GDPR terms that must be known: data subject, controller, and processor. The data subject is the actual end user that the GDPR data is associated with. The controller is the entity that interfaces directly with the data subject for the purposes of performing some function that falls within GDPR. Lastly, the processor is the entity that "processes" the GDPR data on the behalf of the controller. Keep in mind that if the controller doesn't outsource the processing then the controller would fall into both categories. You can also have situations where the controller outsources the processing who, in turn, outsources to another processor. GDPR has special provisions for such an occasion and this should be closely investigated before allowing.

While some companies may have started sooner, the experience of OpenSky thus far is that most companies are far behind the power curve and most likely won't make the deadline.

Primarily, a consistent trend that we are seeing as a deficiency, as well as playing a key role in the success of GDPR, is reduction of GDPR producing data sources and accurate application data mapping. As a most basic foundational task, application data mapping must be done in order for companies to be successful with specific GDPR articles.

In relation to GDPR producing data sources, a common theme among our clients is that there are numerous applications that perform the same or similar function. Each application is a GDPR producing data source that would have to be fully mapped out, be considered in relation to privacy impact, ensure full compliance with notice and consent, and appropriate security controls applied in order to protect the data. Obviously, protecting the data protects the controller and reduces risk as well.

Data mapping must be performed accurately and completely. Our experiences thus far are that data mapping is inaccurate and incomplete. To gain the benefits of fully mapping an application, the application owner should work with the infrastructure and security teams to get as much of a complete view as possible. The ideal application data map will show the user interface, any relevant security controls (encryption for example), any network related information such as protocol or port number, the complete path the data takes all the way down to the method of backup and including which tape the data is on while stored offsite.

As previously mentioned, application data mapping is key and a higher number of GDPR producing data sources will only increase the work load of performing the mapping as well as increase the effort and cost to protect those applications. Data mapping is also the primary task that will allow for success in data subject inquiries, auditing, and record keeping. Remember, GDPR is based around increased rights for the data subject rather than the entity that deals with the GDPR data. This means that if the data subject exercises those rights and you can't comply with a simple inquiry then your company may be at great risk of a supervisory authority conducting a GDPR related investigation.

For more information, contact OpenSky at info@openskycorp.com.