Finally, EU officials agree on new data protection reform

Dominic A. Paluzzi, James J. Giszczak | Monday, December 21, 2015

The European Commission announced it reached an agreement to reform the 1995 Data Protection Directive with language for the European Union's new General Data Protection Regulation (GDPR). The reform was years in the making, which made the Commissions' announcement last week a nice holiday present for those of you in the data privacy community who have been waiting on a final resolution.

The final, approved GDPR is available on the European Parliament website. The most important element is that it would establish one set of rules for companies that have to deal with a significant amount of red tape and hurdles when processing personal data on EU data subjects. Currently, there is a patchwork of laws within the EU as each member state was free to enact its own data protection laws. A single law set of rules would make it much easier and more cost-effective for companies to do business in the EU and it would streamline issues through a single supervisory authority.

WHAT WE KNOW IS INCLUDED

1. The General Data Protection Regulation. This will enable people to better control their personal data. Additionally, the modernized and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust.
2. The Data Protection Directive. This is for the police and criminal justice sector and will ensure that the data of victims, witnesses, and suspects of crimes are duly protected in the context of a criminal investigation or a law enforcement action. At the same time, more harmonized laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe.

The chart below summarizes some of the key aspects of the regulation that have been decided upon:

One-stop-shop	Organizations subject to the regulation would only have to deal with a single supervisory authority, not the authority of numerous individual states. This should streamline the process and decrease the number of contacts multinational organizations have with various member states' data protection authorities (DPAs). Under the regulations these organization would only have to deal with the DPA in the member state where the organization is established.
"Right to be forgotten"	EU data subjects will be able to demand that an organization delete all personal data that the organization holds related to them, subject to some exceptions.
Breach notification	Upon discovery of a breach, data controllers must notify each relevant DPA where the breach is likely to cause a degree of risk to the data subjects, within 72 hours. Notice to affected individuals is required without unreasonable delay.
Age of consent	States would be able to set their own age of consent for children to use social media, so long that the limit is between 13 and 16 years of age.
Data portability	Organizations that have EU data subjects who want to switch service providers will need to make it easier for them to transfer their personal data to another service provider.
Fines	Companies may be fined up to 4 percent of their annual global revenue for violations of the regulation. These heavy fines, however, would be reserved for repeat and egregious violations.

WHAT DOES THIS MEAN FOR U.S. COMPANIES?

Unfortunately, any organization that offers any services to EU data subjects is covered by the new GDPR, even if located elsewhere. The 72-hour breach notification requirement alone is enough to cause significant changes in the way that U.S. companies respond to data breaches and compromises of personal information, especially if the breach involves personal information of both U.S. and EU individuals. In addition, unless an organization meets the EU's definition of a small and medium-sized enterprise (SME), that business will be required to appoint a data protection officer (DPO) and perform privacy risk assessments. If personal data processing is a core business activity of the organization, many of the requirements will also apply to SMEs. Finally, the fines for non-compliance – up to 4 percent of the organization's annual global revenue – are the heftiest among all other privacy laws.

NEXT STEPS

The final text of the regulation must still be voted on by the EU Parliament's Civil Liberties Committee. If it passes, it would then have to be approved by the entire Parliament in January 2016. If approved, the regulation would become effective in 2018.

If your company process personal data on EU data subjects, you should start planning for the reforms and determine how to effectuate compliance by the 2018 effective date. You should be taking a very close look at your incident response plan and incident response team to see what needs to be revised as a result of the GDPR. Implementing a plan to comply with the 72-hour breach notification requirement and appointment of a DPO should be at the top of your "to do" list for early 2016.

Should you have any questions or concerns about the regulation or the status of the proposed U.S. laws, please contact one of our data privacy professionals. As always, we will continue to keep you updated on any developments with this and other data privacy news.

For more information, please contact one of the attorneys listed below.

Dominic A. Paluzzi

James J. Giszczak