Data Security: The General Data Protection Regulation (GDPR)

Policy Brief ::: Last Updated 5.24.18

TL;DR

The General Data Protection Regulation (GDPR) goes into effect on May 25, 2018. The GDPR gives users of digital platforms more transparency and greater control over how their personal data is used. Lawmakers posit that increased access will improve consumer trust — an essential component to encouraging growth within today's digital economy. As the first prominent data privacy law of its kind, the GDPR holds global significance. Numerous countries are looking to the European model for crafting their own data protection laws. The GDPR is relevant for U.S.-based companies, too. Any company that collects, processes, or analyzes data tied to individuals in the EU must comply with the regulation by, among other things, implementing processes that ensure compliance: requiring regular training, auditing, and updating of privacy policies.

Summary of GDPR

The General Data Protection Regulation (GDPR) was adopted by the EU on May 25, 2016 and goes into effect on May 25, 2018. The GDPR applies to the processing of personal data by public and private authorities for commercial and daily activities — not for law enforcement agency (LEA) purposes. A separate law, the Police Directive, sets the rules that LEAs have to follow when processing data during court proceedings and investigations. The GDPR's impact is not in the data protection rights, which EU users have largely enjoyed since 1995, but in the stronger enforcement mechanism which includes fines of up to four percent of the offending company's global turnover, in cases of repeated violations of users' rights. These fines are imposed by Data Protection Authorities (DPAs), which every member state must appoint.

The powers of the DPAs are also increased: all are allowed to conduct investigations, or investigations can be mandated by consumer organizations when they represent citizens. The GDPR also codifies data protection into law in very general terms while harmonizing data breach notification requirements. Of note, users must be notified within 72 hours if a breach affects their rights, and importantly, they can seek remedy. Additionally, companies will be required to hire a

Data Protection Officer, whose sole responsibility will be to oversee a company's data protection strategy and ensure compliance with GDPR requirements.

The GDPR is not limited in scope to the EU, and it has the potential for broader global impact. Already, many countries are looking at EU models when adopting data protection laws, potentially making the EU an international standard-setter. Additionally, the GDPR is important for countries who are seeking membership within the EU — they will need to have data protection laws offering a similar level of protection.

Member Impact

Reverberations from the GDPR will be felt immediately in New York. Any company that has European consumers should be prepared to comply with GDPR provisions.

Today, data security is of critical importance for consumers and businesses alike. Both suffer when there is a cyberattack. Implications of the GDPR should have a positive impact on the protection of both New York's residents and the tech ecosystem at large. Data breaches and identity theft are a threat to everyone, and proactive steps to protect personal information are crucial to ensuring security in the digital age.

Moving Forward

We support efforts that protect people's data privacy, but before New York State introduces any legislation similar to the GDPR, there are three things we must consider:

1. *Patchwork, state-by-state legislation may be disastrous.* A single, unifying, federal piece of legislation would likely better serve individuals and prevent miscommunication or confusion among inter-state company dealings.
2. *Cultural inconsistencies exist.* The GDPR was built within the culture of a continent that is quite different from that of the U.S. For example, the "Right to be Forgotten," in place in the EU since 2006, establishes individuals' autonomous agency to claim removal of their name alongside certain keywords in search engine results. This type of erasure may run contrary to interpretations of freedom of expression, the right to privacy, and other issues of censorship in the U.S.
3. *Hurry up and wait.* The GDPR will take effect on May 25, 2018. It is entirely appropriate to wait and see what implications it will create. Holding legislative action to gauge what components are and are not meaningful will likely save future legislative overhaul.