GDPR Enforcement Begins Friday: 4 Things You Need to Know

May 22, 2018

1. What is the GDPR?

The GDPR is the European Union's General Data Protection Regulation, a comprehensive set of strict privacy laws and regulations. The EU passed GDPR in 2016, but granted a two-year grace period which ends this Friday, May 25, 2018.

The new regulations governs how organizations collect, store, use, process and transfer the personal data of EU residents, giving them more power and control than ever before. It treats data privacy as a fundamental right for individuals in the European Union.

2. The GDPR is an EU regulation, why do I care?

Extraterritorial Reach. The GDPR's reach is not limited to EU territory. It applies to any organization located in the EU or that stores EU resident personal data in the EU. The GDPR also applies to organizations outside the EU that target goods or services to the EU or track the activities of EU residents.

Broader Definitions. "Personal data" means any information that could lead to the identification of an individual EU resident. It can include just a person's name (if sufficiently unique), a photograph or image, a computer's IP address, or a social media post. "Processing" personal data includes almost any activity, including just holding it.

Targeting Activity. Under the GDPR, it matters how and to whom you market. If you operate a US website (with a German language version) that sells lederhosen in both dollars and Euros to Germans, Austrians and the Swiss, you must comply with the GDPR for the personal data you collect from your European customers. If your US website uses only English and dollars and only occasionally ships products to Europe, you are not likely "targeting EU residents" under the GDPR.

Tracking Activity. Just because your website does not target the EU, however, does not mean you can ignore the GDPR. If your US website uses analytics (like Google Analytics) to track the behavior of visitors to your website and you capture the activities of EU residents and use that data to individually tailor the website to those visitors, you may be "tracking EU residents" subject to GDPR regulation.

Fines. The penalties contemplated by those regulations are harsh. Failure to comply with the requirements of the GDPR can result in fines of the greater of €20 milllion or 4% of global turnover—whichever is greater.

3. What individual rights does the GDPR establish or protect?

- *Minimal, Purposeful Collection with Notice.* You must collect only the personal data necessary, and only for identified purposes. You must use it only for those purposes.
- *Lawful Use.* Your use of the personal data must be both lawful and fair to the individual's interests.
- *Minimal Storage.* You must store personal data only when necessary, and only for as long as it is useful to the purpose it was collected.
- *Consent.* In general, consent under the GDPR must be a knowing, affirmative "opt-in," not an "opt-out."
- *Erasure.* When requested by the individual, you must completely delete his or her personal data.
- *Accuracy.* You should maintain accurate and up-to-date personal data.
- *Integrity and Confidentiality.* You are required to maintain the integrity and security of the personal data, and keep it confidential.

4. What should I do now that the GDPR is here?

You should have someone in your company who can find out what personal data you collect, what you do with it and how you protect it. If the GDPR applies, you will need to review your legal basis for processing the data, and have a method in place to respond to and document requests by individuals to see, correct or delete their personal data.

Enforcement by the new European Data Protection Board (EDPB), together with local EU data protection authorities, will be largely complaint-driven. In all likelihood, companies with EU operations, lots of EU personal data, or clearly non-compliant activity will be the first scrutinized. Still, the GDPR has been pending for two years, and the EU is taking the GDPR seriously.

Some of your customers may have sent you a GDPR due diligence questionnaire or proposed a Data Transfer Agreement regarding the personal data entrusted to you. If you have not received such requests, you soon will. Those customers and business partners expect you to know your obligations under the GDPR, and will seek to hold you liable if you breach them.

If you have EU locations, employees, or vendors/suppliers, if you target or track EU residents, or if your customers are insisting on GDPR compliance, you need to take stock of the personal data in your possession. The rest of the world is heading toward GDPR-like regulation of personal data. May 25th should serve as a wake up call for those businesses who have yet to consider GDPR's consequences.

Let the cybersecurity/data privacy professionals at Lathrop Gage, Tedrick Housh and Jason M. Schwent, assist you with any of your GDPR compliance questions or concerns.