U.S. Companies with Global-Reach Take Note: GDPR is on the Fast-Approaching Horizon

Amundsen Davis Data Privacy & Security Alert
May 21, 2018

On May 25th, a monumental data-breach land shift will occur. As the U.S. kicks-off Memorial Day celebrations, residents of the European Union will enjoy the first days of enforcement of the EU's General Data Protection Regulation (GDPR).

Did you know? Are you ready? Maybe not. U.S. companies—if they even know about the GDPR—may have turned a blind eye with the thought, 'this doesn't apply to me.' Not (necessarily) so. In fact, a company's lack of compliance could land it in scolding hot water. This is because the GDPR packs an eye-popping financial punch (see below) and applies to any organization that "processes data" of any individual in the EU (citizens, residents and visitors) as well as EU citizens living abroad, *regardless of the organization's location*. It applies to your virtual presence as well. So, any U.S. company that has a web presence (and who doesn't?) and markets their products over the web should take notice.

What is the GDPR? It's a law that protects data and privacy for European Union residents. Its reach is broader than the "typical" personally identifiable information (known here as PII) because private information includes names, addresses and ID numbers together with web data such as location, IP address and cookie data. U.S.-based hospitality, travel, software service and e-commerce companies should be ready. Indeed, any U.S. company that has identified a market in an EU country and has localized web content should review their web operations.

In practical terms, companies need to ensure that EU-directed online marketing forms and interactions are adjusted to obtain explicit consumer consent. For instance, if an EU customer signs-up for a service or buys something, you need to obtain express permission for *each* type of processing done on the data (i.e., email promotions or sharing with third-party affiliates). Once the data is collected, you need to protect it. This means having data security standards (like ISO 27001 or NIST standards) in place. If something happens, you need to react quickly. GDPR contains a 72-hour breach notification rule.

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

U.S. Companies with Global-Reach Take Note: GDPR is on the Fast-Approaching Horizon

Companies simply cannot conclude 'this will never happen to us' or continue to believe they are only accountable for actual breaches. Noncompliance with GDPR's code of practice could translate into an organization facing fines of up to 2% of their annual turnover or €10 million, whichever is higher. A single breach of people's personal data could mean as much as 4% of your annual turnover or more than $23 million, whichever number is higher. There is a safe harbor—fines must also be "proportionate"—however, if you cannot prove you've made any effort to comply with GDPR and look ignorant of the law, you can expect a steep fine.

So, what can you do? At a minimum, take the following steps:

1. Document the personal data you hold;
2. Honor citizen's data requests (including deletion, amendments, or transfers of that data);
3. Establish a lawful basis for processing data (and you may want more than one);
4. Audit (or establish) your data breach response plan to ensure compliance with the GDPR 72-hour notification rule;
5. Appoint a data protection or privacy officer.

U.S. companies are not immune to the consequences of the EU's enforcement of GDPR and should take precaution.