DYKEMA

Issues Brief

Does the EU's GDPR Apply to Your Company?

The European Union's General Data Protection Regulation (GDPR) takes effect May 25, 2018. The GDPR will affect companies all over the world, regardless of whether they are located in the EU. Many US-based companies are surprised to find they must also comply or risk facing large fines. If these regulations apply to your company now, or may in the future, you can't afford to wait. Do they apply to your company? If so, are you ready? Find out below:

Does your company have any employees in the EU or UK?

Does your company offer a good or service to someone in the EU or UK?

If you answered yes to either of these questions, you need a GDPR compliance program!

What is personal data?

The GDPR protects "personal data," which is any information directly or indirectly relating to an identifiable person (aka "data subject"). This includes: a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. It does not matter if the data subject has ever purchased your company's product or services.

But I only do business in the United Kingdom. Will Brexit save me?

No. The UK will still be a member of the EU when the GDPR take effect in May. But even after it leaves, the UK has stepped up efforts to adopt regulations consistent with the GDPR in order to preserve continuity of data with key trade partners. In fact, the UK's proposed Data Protection Bill, when adopted, might even go a little further than the GDPR.

What does it mean to "process" data?

The GDPR defines "processing" very broadly, so as to capture virtually any use of data, describing it as "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Put another way: If you have a contact list, you process data under the GDPR.

Controllers, processors … what are these?

A data controller is defined as a party that "determines the purposes and means of" personal data processing. A data processor is a party that does the actual processing. Both are regulated by the GDPR.

Compliance Programs

So the GDPR applies to your company. What does this mean?

First, you'll need to create a compliance program to protect yourself in the event of a data breach or other violations. Penalties for violating the GDPR include fines up to the greater of €20 million or four percent of your company's annual worldwide revenue. Here are the basics about the regulations:

Purpose and Use Limitations

Unlike the US, the GDPR severely limits how much information you can gather, what you can do with it and how long you can keep it.

Consent

How important is it for controllers and processors to develop an effective consent management program? The EU's own website describes "not having sufficient customer consent to process data" as an example of the most serious GDPR infringement that would warrant the its largest fine.

Impact Assessments

Data controllers must carry out an impact for any data processing activities that may significantly affect a data subject's rights under the GDPR. Examples of these activities include using new technology to process data, and using automated processing and high-volume processing of sensitive data.

Privacy-by-Design

Privacy-by-design requires the data controller or processor to protect personal data by ensuring that privacy is the default setting in all new products.

Data Breach Notifications

Data controllers must report any breach to a Supervisory Authority and affected data subjects "without undue delay"—within 72 hours if feasible —unless the breach is unlikely to put the subjects' rights and freedoms at risk.

Data Transfers

GDPR privacy protections follow the data. Therefore, most data transfers from the EEA are prohibited without proper legal protections in place.

Data Protection Officers

Some data controllers and processors will need to appoint a Data Protection Officer to keep internal records of its data processing activities. These organizations are:

- Those whose core activities involve processing operations which require regular and systematic monitoring of data subjects on a large scale.
- Those processing special categories of data or data related to criminal convictions and offenses.

Security

Data controllers must take security measures "appropriate to the risk" to protect data, including pseudonymization and encryption. Pseudonymization means processing personal data so that it can no longer be attributed to a person without additional information.

Dykema's Data Privacy and Data Security Practice regularly counsels clients with creating compliance programs to protect data against the world's most dangerous threats. Our lawyers can help audit your data to determine potential GDPR liability and develop a comprehensive compliance program.

Erin F. Fonté
Austin, TX
512-703-6318
efonte@dykema.com

Cinthia Granados Motley
Chicago, IL
312-627-2107
cmotley@dykema.com

DYKEMA

www.dykema.com

California I Illinois I Michigan I Minnesota I Texas I Washington, D.C.