A New European Data Breach Regulation is Coming

The European Union has enacted a comprehensive and far-reaching data privacy initiative known as GDPR that is set to go into effect soon and contains massive penalties for non-compliance. How could it affect US businesses? Let’s take a look at some common questions.

What do the initials “GDPR” stand for?
“General Data Protection Regulation” (Eugdpr.org)

My clients and myself are all based in the United States. Do US-based businesses care about this?

Yes. Even if the company does not have a business in the EU, the regulation can apply if:

• The business offers goods or services to EU subjects regardless of whether payment is required.
• The business monitors the behavior of EU subjects. (Clicking on social media links, analyzing marketing likes/dislikes).
• The business stores and holds the personal data of EU subjects.

Can you give me a quick idea of what this new law is about?

The GDPR unifies data protection laws for “Personal Data” across the European Union with the intention of strengthening privacy rights of consumers. It imposes hefty fines on companies that don’t comply. The GDPR has many requirements, but here are the primary ones:

• The personal data you collect must be “minimized, accurate and portable.”
• You need to obtain informed consent from a EU consumer before collecting, storing or using their personal data.
• Their personal data must be “provably deleted” if the consumer so chooses.

Who is affected?

Any US business that offers goods or services to customers in the European Union or holds any personal data on European Union subjects.

When does this new law take effect?

May 25, 2018
What does the new law consider “Personal Data”?

- Name
- Address
- Photo
- Email Address
- Financial information
- Healthcare information
- The law also includes data that could indirectly identify an individual (racial or ethnic origin, political opinions, religious beliefs, etc.)

What does GDPR say a business must do if they are the victim of a data breach?

The GDPR requires that companies notify individuals of a breach of their personal data. Notification must include:

- The name and contact information of the company’s data protection officer
- The anticipated consequences of the breach
- Any measures taken by the company to remedy or mitigate the breach

What are the penalties if a US business doesn’t comply with GDPR?

The monetary penalty is €20 million or 4% of a company’s annual revenue, whichever is greater.

What should US businesses do now?

Here is a great resource to review: Dacbeachcroft.com. And if you or your clients have not purchased a comprehensive Cyber Liability insurance policy, it should be considered now. If you or your clients have purchased Cyber Liability, it is important to understand how the carrier is/is not addressing GDPR fines & penalties and what their respective policy triggers are.