GDPR Compliance 101 for US Companies

Why Does a US Company Need to Prepare for GDPR?

The GDPR is an EU law, so why does a US company need to prepare for GDPR implications? To answer that, let's first see exactly what it is.

Online collection and use of personal information began in the 1990s and has since become simply the norm for online businesses. Even after online data collection's explosive growth and becoming a commonplace practice, most consumers are still unaware of the huge amount of personal information collected and exactly how it is used.

GDPR Overview for US Companies

So here's a quick overview concerning GDPR compliance for US companies.

Two overarching points to keep firmly in mind concerning the GDPR obligation for US companies are laid out in a Forbes piece.

First, "Article 3 of the GDPR says that if you collect personal data or behavioral information from someone in an EU country, your company is subject to the requirements of the GDPR," but only if the person is actually "in the EU when the data is collected."

GDPR Fines for US Companies

As we mentioned, one of the main points of the GDPR is a system of fines for noncompliance. It's not exactly clear yet how the system of GDPR fines can and will be enforced and fines collected in countries outside the EU. But the fines are not insignificant.

Each EU member state must designate an authority for data protection in order to enforce the GDPR. In the case of a data breach or proven GDPR noncompliance, a business can be fined **20 million** Euro ***(around US$23.5 million)*** or up to **4%** of global annual revenue, whichever is greater.

GDPR Requirements for US Companies

The GDPR requirements for US companies are pretty straightforward. Still, there are some size differences to be aware of because GDPR compliance for small US businesses is less extensive than for larger businesses.

Consent is one of the foundational aspects of the GDPR, so you have to ensure that you obtain user consent for every kind of collection and use of personal data in every instance.

GDPR Compliance Checklist for US Companies

To make this all a little easier to grasp at a glance, here's a GDPR compliance checklist for US companies ***(taken largely from NG Data)***:

Sample GDPR Policy for US Companies

Data Protection Policy
An essential guide to employees regarding how they may use data, how they can keep it secure, and the consequences of misuse. A good Data Protection Policy can prevent data breaches by helping employees understand how they are supposed to handle data.

Data Retention Policy
A statement explaining when data in documents (or data held electronically) should be deleted. This policy sets out the time limits for deleting different types of documents so that we can stay within the GDPR storage limitation principle found in Article 5 of the GDPR.

Data Breach Incident Policy
An emergency plan that tells your company what to do if a data breach occurs, how to form a team to deal with the breach, how to prevent any further loss of data and whether the company needs to tell customers and Regulators about the breach.

Some ancillary elements are

Compliance Costs for GDPR

What are the compliance costs for GDPR? Well, there are two ways to look at it. You could see it as fairly costly in terms of labor and technical adjustments. Or you could view is as very inexpensive and worth every penny if it helps you avoid the fines. So here's how it works out.

The largest portion of the costs will be in auditing and classifying the held data, but this is a step that simply can't be neglected.

Act Now for US GDPR Compliance

Doing everything possible to ensure GDPR compliance for US companies is now an absolute must – and a pretty urgent one for many of them. The team at Fingerprint Marketing can be that third-party expert you need to be compliant.

FINGERPRINT MARKETING
Leave your mark.
10400 NE 4th St Suite 670, Bellevue, WA 98004
(425) 283-3943
www.fingerprintmarketing.com.