Logistics Marketing Advisors

GDPR Basics

Understanding the GDPR

GDPR, or General Data Protection Regulation, legislation has been created to give people (or *data subjects*) more control over their personal data and regulate how this information can be collected and used. This "personal information" encompasses the usual suspects like name, address, and social security number (or equivalent), but also covers a wide range of items including religion, ethnicity, IP address, mobile device ID, genetic information, social media posts, and marital status, to name a few.

Principle	Explanation
Lawfulness	Data should be processed only when there is a **lawful basis** for such processing (eg, consent, contract, legal obligation)
Fairness	The organization processing the data should provide data subjects with **sufficient information** about the processing and the **means to exercise their rights**
Transparency	The **information provided** to data subjects should be in a **concise and easy-to-understand format** (eg, the purpose of consent should not be buried in a lengthy document of terms and conditions)
Purpose limitation	Personal data may be collected only for a **specific, explicit, and legitimate purpose** and should not be further processed
Data minimization	The processing of personal data should be **adequate, relevant, and limited to what is necessary** in relation to the purposes for which those data are used
Accuracy	Data should be **accurate and kept up to date**
Storage limitation	**Data should not be held** in a format that **permits personal identification any longer than necessary**
Security	Data should be processed in a manner that **ensures security and protection against unlawful processing, accidental loss, damage, and destruction**
Accountability	The **data controller** is responsible for **demonstrating compliance**

Source: McKinsey&Company. https://www.mckinsey.com/business-functions/risk/our-insights/tackling-gdpr-compliance-before-time-runs-out

Under the GDPR, data subjects have the right to access information that companies have about them, as well as the right to have their data removed ("the right to be forgotten"). Businesses, on the other hand, are forced to comply with new requirements related to the collection and handling of personal data (see graphic inset right for details on the GDPR's guiding principles).

The legislation, however, doesn't speak of "businesses" but of "controllers" and "processors" that collect personal information from EU citizens and/or offer products or services to EU citizens.

A data *controller* is the entity that determines when and where a data subject's information is collected and the way that it is used. A data *processor* is the entity that captures, manages, or otherwise handles the data on behalf of the controller. For example, a controller can be a company that sells its products to customers and collects personal information to do so. It then shares that information with vendors (i.e., processors) that use that information to ship the order and receive payment.

Does the GDPR affect U.S. companies?

Importantly, your business does not have to physically reside within the EU to be affected by the GDPR; it simply must meet one or both of the following criteria:

- Do you collect personal data from EU citizens?
- Do you offer products or services to EU residents?

If you answer "yes" to one or both questions, then consider yourself affected.

However, there's another way you might be affected by GDPR: your customers' contracts may stipulate that you need to be compliant or lose the business. This is becoming increasingly common in industries such as logistics, eCommerce, travel, and software services.

How do you comply with GDPR Legislation?

Once you realize that your business is, in fact, affected by GDPR, it's time to comply. The costs of not doing so are simply too high. In addition to the potential lost business from customers who demand that you adhere to GDPR, the EU promises to issue severe penalties for non-compliance. These penalties can be as high as $23 million or $4 percent of annual revenue, whichever is greater.

Now, the EU is not rolling this out and immediately penalizing offenders left and right. There will likely be a long sequence of warnings and slaps on the wrist before any substantial fines are levied. Frankly, there is a question of whether these fines can be successfully levied in the first place. As of this writing, the answer to that is unclear. However, it's probably not a good idea to be the company in the headlines who will find out for the rest of us.

So, on to compliance.

The full GDPR document is 88 pages long. Here are some basic tips that summarize a company's requirements under the law. NOTE: we are not lawyers nor experts on GDPR, so our thoughts are not meant as legal advice.

Audit your data management systems. You need to have full understanding of your data: what you store, where it came from, the various places it can be accessed, and who you share it with. Under the GDPR, users can request that you provide them with records of their personal data. They can also request that you remove their data from your systems completely. Can you comply with each request?

Audit the data management systems of your vendors. If you share data with third-party vendors, such as a CRM or marketing automation provider, non-compliance in their systems can harm your business just as much as your own non-compliance. Review your providers' data management infrastructure and evaluate your service-level agreements to find potential GDPR-related issues and opportunities for improvement.

Protect against data breaches. Ensure that you have the systems, personnel, policies, and procedures in place to both prevent data breaches and report them should they occur.

Update your privacy policy. A Privacy Policy is where you let your users know:

1. What personal information you collect
2. How and why you collect it
3. How you use it
4. How you secure it
5. Any third parties with access to it
6. If you use cookies
7. How users can control any aspects of this

Along with the seven standard points above, you must also include the following information in your Privacy Policy to be GDPR-compliant. Note that each point doesn't have to be a separate clause. If the information is somewhere in your policy, it will work.

1. Who your data controller is (the data controller will likely be your business, unless your business operates as a data processor for other companies)
2. Contact information for the data controller
3. Whether you use data to make automated decisions (e.g., loan screening or employment decisions)
4. Inform users of the 8 rights they have under the GDPR
5. Whether providing data is mandatory (if so, what happens if they don't provide it?)
6. Whether you transfer data internationally
7. What your lawful basis is for processing data

Determine your lawful basis for storing user data. Under the GPPR, businesses need a legal reason (or "lawful basis") to use the data of an EU citizen. There are six legal reasons, including:

- *Consent:* The person consented to have information stored and/or to be contacted after being clearly informed about what he or she was opting into.
- *Performance of a contract*: Businesses can store information and contact individuals in accordance with a contract (e.g., sending a customer a bill).
- *Legitimate interest*: This is the most subjective item of the six. Examples of this legal reason include contacting a client or sending a direct marketing message to an existing customer about a product or service similar to the one the customer has already purchased.

Get consent. In general, you should ask for consent whenever you collect information from a user (e.g., have user check a box or click a button to enroll in a blog subscription instead of auto enrolling) and inform the user about what you will do with that information. You also need to notify users, in plain language, if you are using cookies on your website (see examples). The user will then need to consent, typically by checking a box. If your website operates on a platform like HubSpot or WordPress, there are a variety of tools to make all consent-related tasks simple to implement.

With the GDPR legislation now in effect, the time to address your company's compliance is now. Get input from your IT and legal teams to ensure you're covering all necessary bases. But, it is a requirement that, when met, will not only have your business up-to-date with key legislation, but will also strengthen the security of your data and make your data management capabilities more transparent to prospective customers.