Cyber News Brief

COMPLYING WITH THE GDPR

Most businesses view their customers' personal data as a digital commodity that can help with marketing, customer retention, analytics and more. However, the European Union's (EU) upcoming General Data Protection Regulation (GDPR) comes into force on **May 25, 2018**, and will require businesses to give EU citizens much more control over their personal data.

The GDPR applies to any organization that operates in the EU or manages EU-based data. Unfortunately, standard cyber security measures likely won't be enough to comply with the rule, as U.S. regulations usually only require businesses to protect data such as financial or medical information, and the GDPR's definition of personal data is much broader.

Any business that fails to protect personal data and comply with the GDPR could face major fines. However, complying with the rule could attract customers who value privacy and give businesses better insight into their data management procedures. As a result, it's crucial to understand the GDPR's requirements and the steps needed to stay compliant.

What Counts as Personal Data?

Under the GDPR, personal data counts as any information relating to an identifiable person. Essentially, any information that could potentially lead to a person's identification can be considered personal data. Here are some examples of personal data under the GDPR:

- IP addresses
- Internet cookies
- Email addresses
- Any location information
- Medical data, including genetic and biometric data
- Because the GDPR applies to a broader range of data, businesses need to be especially careful when examining their data management procedures.

Compliance Requirements

Any violation of the GDPR can be financially devastating, as fines can reach as high as €20 million (almost $25 million) or 4 percent of a company's global annual revenue.

In order to protect your business, it's important to keep these five key features of the GDPR in mind:

- **Requirements for controllers and processors**—The GDPR defines two distinct types of operators in its regulations—controllers and processors. The following are general definitions and standards that apply to these entities:
    - **Data controllers**—Under the GDPR, any organization that collects, uses or discloses the personal information of EU citizens may be considered a data controller. Controllers must protect EU citizens' data and ensure that the organizations that process personal data on their behalf also comply with GDPR requirements. Controllers must conduct privacy impact assessments for any high-risk processing and maintain records of all processing activities.
    - **Processors**—Data processors are the organizations that actually process data on behalf of controllers. These entities must also implement appropriate safeguards, return or delete data once processing is complete, and notify the controller of any data breaches. Processors cannot subcontract any tasks without a controller's permission.
- **Lawful bases and consent requirements**—Data controllers can only process data under one of the GDPR's six lawful bases:
    1. Consent from the data subject
    2. Contractual necessity
    3. Compliance with legal obligations
    4. Protection of a data subject's or another person's vital interests
    5. Actions that benefit the public interest
    6. Actions for a business's legitimate interests

  Additionally, a data subject's consent must be unambiguous—silence or inactivity does not constitute consent. Parental consent is required when organizations process data for individuals under the age of 16.
- **Mandatory data breach notifications**—After a data breach is discovered, data controllers must notify all affected individuals **within 72 hours**. However, when a breach could potentially affect individuals' rights or freedoms, the notification

must be made immediately. Data processors must also report breaches to data controllers.

- **Right to erase**—Data controllers are required to erase processed and/or stored personal data under the following conditions:
  - The data is no longer needed
  - An individual objects to the processing
  - The processing was unlawful
- **Requirement for data protection officers**—Data controllers and processors may be required to designate a data protection officer in the following scenarios:
  - If data processing is carried out by a public authority or body
  - If core activities involve regular and systematic monitoring of individuals on a large scale
  - If core activities consist of large-scale processing of certain categories of data (i.e., data related to racial or ethnic origins, criminal convictions or political views)

While this list outlines a number of the major considerations, it shouldn't be used as a compliance guide. To review the full text of the GDPR, helpful FAQs and summaries of key provisions, visit the EU's official website.

Creating a Compliance Plan

Because businesses can collect, manage and store data in different ways, it's important for your GDPR compliance plan to include details that are unique to your organization. Here are some of the most important topics to consider when making your plan:

- **Conduct a readiness and data assessment.** Review the GDPR and determine if it applies to your business. You should also establish what personal information you collect, where it's stored and who has access to it in order to identify what data applies to the GDPR.
- **Identify compliance gaps.** During your initial assessment, it's important to identify any potential compliance gaps. In some cases, you may find that you are able to reduce your GDPR compliance burden by changing the way you store or track EU data.
- **Establish oversight.** Continually document, model and coordinate potential GDPR issues and remediation strategies. You should make this information readily available to any employees who may handle personal data.

> **Implement a GDPR compliance program.** After you've established key processes to identify compliance gaps, create a GDPR program to address potential concerns. This program should account for the following:

- Governance
- Policy management
- Data life cycle management
- Individual rights processing
- Information security
- Data breach management
- Data processor accountability
- Training and awareness

> **Examine your vendors' and partners' data management practices**. Make sure that business partners such as cloud service providers, payment processors and marketing firms are ready to comply with the GDPR. Even if your own data protection measures are in place, you can still be held partially liable for a vendor's failure to comply.

Review Your Cyber Risk Management Program

Organizations process massive amounts of personal data every day and expose themselves to risks from cyber attacks, data breaches and more. Just one breach can result in serious damage to your finances and reputation.

To better protect your organization, it's important to speak with a qualified insurance broker and improve your cyber risk management program. Not only can brokers provide general guidance on any applicable data breach laws, they can also help you round out your risk management programs with custom insurance policies. To learn more, contact MJ Insurance today.

The content of this News Brief is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and should not be relied upon as such. © 2018 Zywave, Inc. All rights reserved.