What Is GDPR?

A Guide to the EU's General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a regulation the European Parliament, the Council of the European Union and the European Commission established in order to strengthen and unify data protection for all individuals within the European Union (EU).

It also addresses the export of personal data outside the EU. The GDPR's primary goal is to give citizens and residents control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR took effect on May 25th, 2018, it replaced the Data Protection Directive (officially Directive 95/46/EC) of 1995. Unlike a directive, the GDPR does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

GDPR is now the primary law regulating how companies protect EU citizens' personal data. Companies must now ensure that they're compliant with the new requirements of the GDPR or be subject to stiff penalties and fines.

Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders

Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Simply put, the GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

WHO IS SUBJECT TO GDPR COMPLIANCE?

Although the purpose of the GDPR is to impose a uniform data security law on all EU members so that data protection laws are consistent across the entire EU, it's important to note that any company that markets goods or services to EU residents, regardless of its location, is subject to the regulation. That means that U.S. companies doing business in the EU must also become GDPR compliant.

GDPR requirements apply to any organization doing business in the EU or that processes personal data originating in the EU, be it the data of residents or visitors. So, organizations of any size in any country that process anyone's data—if that data originated in the EU—is subject to the GDPR.

100,000 people in 48+ countries use ShareVault for unmatched document security

If you're a business outside the EU, this can get a little murky. Suppose that you are a US-based company that owns a retail storefront. In addition to retail sales you also have an online presence that allows people to shop for, buy and rate your products. In the course of those activities you collect personal data about the people that visit and make purchases for the purpose of compiling sales reports and conducting more targeted sales campaigns. If a person visits the website while they are physically present in the EU, the requirements of GDPR follow the personal data collected during their visit. That essentially means that any website or mobile application that is accessible by a person in the EU must comply with GDPR.

There are, of course, allowances for small businesses and practical limitations on what the EU will attempt to enforce. But entities located outside the EU that market their products or do business with people inside the EU will need to consider the ramifications of not complying with GDPR.

WHAT ARE THE REQUIREMENTS?

What does complying with GDPR mean to you? The GDPR contains 11 chapters and 91 articles that detail all the technological requirements mandated by the new law with regard to providing notice and managing consent.

PRIVACY AND CONSENT

The regulation states that before collecting personal data, data collectors must create a privacy notice that provides specific information to the data subject. The privacy notice should include information about who will process that personal data, why and for how long the data will be processed, and provide all options the data subject has for managing the processing of their data.

Article 12 of the GDPR law says that this privacy notice should be "explicit," "specific," "informed," and "intelligible." It should be "easily accessible" and use "clear and plain language" to convey all the information required by the law in a form that holds the data subject's interest and allows them to digest the notice. According to Articles 13 & 14 of the GDPR, some items that are required by the GDPR law in a privacy notice include:

- The legal basis on which the data was collected
- A description of what the personal data requested is used for
- Who is collecting the data
- Information on how to reach a data privacy officer of the data collector
- Any data processors the data controller hopes to use
- How long the data controller will keep the personal data, or how that period is calculated
- The request for consent should be clearly distinguishable from other matters
- If automated processing is used the notice should reveal where data subjects may lodge complaints

- The source of data that is not collected directly from the data subject
- The existence of the right to be forgotten
- The right to lodge a complaint with a supervisory authority
- Whether collecting personal data is required or not
- Whether the controller intends to further process the data

The following are some of the chapters and articles that have the greatest potential impact on security operations:

Articles 17 & 18

Articles 17 and 18 of the GDPR give data subjects more control over personal data that is processed automatically. It enables data subjects to transfer their personal data between service providers more easily (also called the "right to portability") and to direct a controller to erase their personal data (also called the "right to erasure").

Articles 23 & 30

Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure.

Articles 31 & 32

Data breach notifications play a large role in the GDPR law. Article 31 requires that controllers must notify Supervising Authorities (SAs) of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach, such as its nature and the approximate number of data subjects affected. Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.

Articles 33 & 33a

Articles 33 and 33a require companies to perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.

Article 35

Article 35 requires that certain companies appoint data protection officers. Specifically, any company that processes data revealing a subject's genetic data, health, racial or ethnic origin, religious beliefs, etc. must designate a data protection officer; these officers serve to advise companies about compliance with the regulation and act as a point of contact with Supervising Authorities. Some companies may be subjected to this aspect of the GDPR simply because they

collect personal information about their employees as part of human resources processes.

Articles 36 & 37

Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.

Article 45

Article 45 extends data protection requirements to companies outside the EU that collect or process EU citizens' personal data, subjecting them to the same requirements and penalties as EU-based companies.

Article 79

Article 79 outlines the penalties for GDPR non-compliance, which can be up to 4% of the violating company's global annual revenue depending on the nature of the violation.

THE RISK of NON-COMPLIANCE

financial_loss.jpgIn comparison to the former Data Protection Directive, the GDPR has much stiffer penalties for non-compliance. SAs also have more authority than in the previous legislation because the GDPR sets a standard across the EU for all companies that handle EU citizens' personal data. SAs hold investigative and corrective powers and may issue warnings for non-compliance, perform audits to ensure compliance, require companies to make specified improvements by prescribed deadlines, order data to be erased, and block companies from transferring data to other countries. For companies that fail to comply with GDPR requirements, fines can be up to 4% of total global annual turnover, or 20 million euros.

CONCLUSION

All organizations, large or small, should be aware of GDPR requirements and ensure they are compliant. For many companies, the first step in complying with GDPR is to designate a data protection officer to build a data protection program that meets the GDPR requirements. By complying with GDPR requirements, businesses will benefit from avoiding costly penalties while improving customer data protection and trust.