GDPR

The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data. Companies that are already in compliance with the Directive must ensure that they're compliant with the new requirements of the GDPR before it becomes effective on May 25, 2018. Companies that fail to achieve GDPR compliance before the deadline will be subject to stiff penalties and fines.

GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. 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?

The purpose of the GDPR is to impose a uniform data security law on all EU members, so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. In addition to EU members, it is important to note that any company that markets goods or services to EU residents, regardless of its location, is subject to regulations. As a result, GDPR will have an impact on data protection requirements globally.

REQUIREMENTS OF GENERAL DATA PROTECTION REGULATION 2018

The GDPR itself contains 11 chapters and 91 articles. 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. The result is that data subjects may transfer their personal data between service providers more easily (also called the "right to portability"), and they may direct a controller to erase their personal data under certain circumstances (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 text. Article 31 specifies requirements for single data breaches: controllers must notify SAs of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it 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 (SAs). 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 international companies 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.

GDPR ENFORCEMENT AND PENALTIES FOR NON-COMPLIANCE

In comparison to the former Data Protection Directive, the GDPR has increased penalties for non-compliance. SAs 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. Data controllers and processors are subject to the SAs' powers and penalties.

The GDPR also allows SAs to issue larger fines than the Data Protection Directive; fines are determined based on the circumstances of each case and the SA may choose whether to impose their corrective powers with or without fines. For companies that fail to comply with certain GDPR requirements, fines may be up to 2% or 4% of total global annual turnover or €10m or €20m, whichever is greater.

BEST PRACTICES FOR GDPR: AN IMPORTANT EU DATA PROTECTION LAW

All organizations, including small to medium-sized companies and large enterprises, must be aware of all GDPR requirements and be prepared to comply by May 2018. By beginning to implement data protection policies and solutions now, companies will be in a much better position to achieve GDPR compliance when it takes effect. For many of these 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.

The General Data Protection Regulation not only applies to businesses in the EU; all businesses marketing services or goods to EU citizens should be preparing to comply with GDPR as well. By complying with GDPR requirements, businesses will benefit from avoiding costly penalties while improving customer data protection and trust.


EST
1993
SPECTRECOM
FILMS