# General Data Protection Regulation (GDPR)

GDPR is a regulation that contains provisions requiring businesses to protect the personal data and privacy of European Union ("EU") citizens for transactions that occur within EU member states including protection of personal data exported outside the EU. Companies need to comply with the regulations by 25th May 2018.

## On whom it is applicable?

Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU. It's a European law, but still several online companies are changing their privacy policies that will apply to all their users globally, irrespective of location. Prior to GDPR, a 1995 regulation, generally applied only if the business was itself physically located, or had processing equipment in Europe. This nexus to physical territory remains, but the GDPR goes beyond, and territoriality is increasingly irrelevant. If your service targets EU residents today, you will be subject to and liable under the GDPR. Many businesses are making some of these safeguards, notably, meaningful notice, consent & opt-out options, available globally rather than adopting country-specific formats. Indeed, developing different technologies with different privacy protections would place a costly burden on companies & developers, it's easier to support just one (high) Global standard.

## What information it protects?

GDPR aims to protect the following information:

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions

- Sexual orientation

## Who within the company is responsible for compliance?

The GDPR defines several roles that are responsible for ensuring compliance:

- **Data controller**: The data controller defines how personal data is processed and the purposes for which it is processed. The controller is also responsible for making sure that outside contractors comply;
- **Data Processor**: Data processors may be the internal groups that maintain and process personal data records or any outsourcing firm that performs all or part of those activities. The GDPR holds processors liable for breaches or non-compliance;
- **Data Protection Officer (DPO)**: The GDPR requires the controller and the processor to designate a DPO to oversee data security strategy and GDPR compliance.

Companies are required to have a DPO if they process or store large amounts of EU citizen data, process or store special personal data, regularly monitor data subjects, or are a public authority. Some public entities such as law enforcement may be exempt from the DPO requirement.

## Penalties for non-compliance

The GDPR allows for steep penalties of up to €20 million or 4 percent of global annual turnover, whichever is higher, for non-compliance.

## How will it affect the companies?

The GDPR requirements will force companies to change the way they process, store, and protect customers' personal data. For example, companies will be allowed to store and process personal data only when the individual consents and for "no longer than is necessary for the purposes for which the personal data are processed." Personal data must also be portable from one company to another, and companies must erase personal data upon request. This process is known as the right to be forgotten. There are some exceptions. For example, GDPR does not supersede any legal requirement that an organization maintain certain data. This would include HIPAA health record requirements.

Several requirements will directly affect security teams. One is that companies must be able to provide a “reasonable” level of data protection and privacy to EU citizens. What the GDPR means by “reasonable” is not well defined. This gives the GDPR governing body a lot of freedom when it comes to assessing fines for data breaches and non-compliance.

What could be a challenging requirement is that companies must report data breaches to supervisory authorities and individuals affected by a breach within 72 hours of when the breach was detected. Another requirement, performing impact assessments, is intended to help mitigate the risk of breaches by identifying vulnerabilities and how to address them.