GDPR

The General Data Protection Regulation (GDPR) is a comprehensive data privacy law that establishes a framework for the collection, processing, storage, and transfer of personal data. It requires that all personal data be processed in a secure fashion, and it includes fines and penalties for businesses that do not comply with these requirements. It also provides individuals with several rights regarding their personal data.

The General Data Protection Regulation is a law that sets guidelines for the collection and processing of personal information from individuals. The law was approved by the European Union in April 2016 and went into effect on May 25, 2018.The GDPR provides consumers with more control over how their personal data is handled and disseminated by companies. Companies must inform consumers about what they do with consumer data and every time that data is breached. GDPR rules apply to any website regardless of where they are based.

GDPR Requirements for Data Controllers and Data Processors

- **Lawfulness, fairness and transparency**: Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation**: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization**: You should collect and process only as much data as necessary for the purposes specified.
- **Accuracy**: You must keep personal data accurate and up to date.
- **Storage limitation:** You may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality**: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- **Accountability**: The data controller is responsible for being able to demonstrate GDPR compliance with all these principles.

In addition to describing these principles in detail, the GDPR requires several specific actions that data controllers and processors need to take. Some of these include:

- **Record keeping:** Data processors must keep records of their processing activities.
- **Security measures:** Data controllers and processors must regularly use and test appropriate security measures to protect the data they collect and process.
- **Data breach notification:** Data controllers that suffer a personal data breach must notify appropriate authorities within 72 hours, with some exceptions. Usually, they also must notify the individuals whose personal data was affected by the breach.

- **Data Protection Officer (DPO):** Companies that process data may need to hire a Data Protection Officer (DPO). The DPO leads and oversees all GDPR compliance efforts.

The full requirements for data controllers and processors are described in the GDPR.

Data Subject Rights Under the GDPR

The GDPR defines a data subject as "an identified or identifiable natural person." Data subjects have the following rights:

- **Right to be informed:** Data subjects must be given easy-to-understand information about how their personal data is collected and processed
- **Right to data portability:** Data subjects can transfer their data from one data controller to another
- **Right of access:** Data subjects have the right to obtain a copy of collected personal data
- **Right to rectification:** Data subjects can correct inaccurate data about themselves
- **Right to erasure:** Data subjects can request that their data be deleted (also called the right to be forgotten)
- **Right to restrict processing:** Under certain circumstances, data subjects can limit the way their personal data is being processed
- **Right to object:** Data subjects have the right to object to the processing of their personal data, and under certain circumstances the data controller or data processor will be obligated to comply with the data subject's objection
- **Right to object to automated processing:** Data subjects can object to a decision that legally affects them that is based solely on automated data processing

Penalties for Violating the GDPR

The GDPR describes the fines that are to be imposed on businesses that violate its policies.

There are two tiers of fines under the GDPR, with each tier corresponding to a different category of violation:

- First tier: A violation results in a maximum fine of either €10 million or 2% of the business's worldwide annual revenue, whichever is higher.
- Second tier: A violation results in a maximum fine of either €20 million or 4% of the business's worldwide annual revenue, whichever is higher.

In addition to these fines, data subjects can seek compensation for damages when a business violates the GDPR.

Cloudflare and data privacy

The Cloudflare mission is to help build a better Internet, and data privacy is core to that mission. Cloudflare builds its products with a "privacy by design" mindset and has released several services to increase user privacy (including the Cloudflare Data Localization Suite). Cloudflare typically acts as a data processor when providing its services (e.g., CDN, DDoS protection, DNS). Customers (usually website owners) are the data controllers who determine the purposes and means of data processing. Cloudflare also has obtained the EU Code of Conduct privacy validation the first GDPR code of conduct officially recognized by the EU.