

What is GDPR?

This law gives consumers more control by requiring their consent for the collection and use of their data. It standardizes a wide range of different privacy legislation across the E.U. into one central set of regulations that will protect users in all member states. The primary goal of the GDPR is to ensure privacy, and security and enable people to have control over their data.

Timeline

- **April, 2016**- Adopted
- **May, 2018**- Came into effect

Enforcement Authority

DPAs (Data Protection Authorities) of the EU are empowered to oversee enforcement of the GDPR, investigate events that are not compliant with GDPR policies, and initiate legal proceedings where necessary.

Who All Need To Comply?

It applies to all organizations, public or private, anywhere in the world-that handle, store or process the personal data of EU citizens.

Consumer Rights

- The right of access
- The right to rectification
- The right to erasure/right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

GDPR Checklist

- **Data Security-**

- 1-Take data security into account when developing a new product
- 2- Encrypt, pseudonymize, and anonymize personal data.
- 3- Data protection awareness amongst the team with an internal security policy
- 4- Dedicated process to notify authorities and data subjects
- 5- Assign a date for organizational data assessment

- **Accountability and Governance-**

- 1- Appoint someone responsible for enabling GDPR compliance across the organization.
- 2- Appoint a DPO (Data Protection Officer) from within one of the E.U. member states.

- **Transparency-**

- 1- Publish a Privacy Policy that clearly explains the use of personal data with a legal justification for all.
- 2- Convey information that educates users on what information your organization processes and has access to it.

- **Privacy Policy and Rights-**

- 1- Customers should have information and access to all their stored data in the organization
- 2- They should be able to rectify that information
- 3- Should be given the option to delete their data
- 4- Customer's consent must be obtained and approved before collecting any data.
- 5- The user can stop an organization's use and collection of their data at any given time.
- 6- The customer's data should be in a format that is easy to review and can be changed or transferred.

We've built a secure and seamless tool to collect and manage your website visitors' consent and preferences, all while being compliant with every global data privacy law. Speak to our data privacy professional today!

***Any information obtained from the Adzapier website, services, platform, tools, or comments, whether oral or written, does not constitute legal or regulatory advice. If legal assistance is required, users should seek legal advice from an attorney, a lawyer, or a law firm.*