

General Data Protection Regulation (GDPR)

The GDPR proposed by the European Commission (EC)



GDPR: Is Your Organization Compliant?



Is your organization compliant to data protection regulations?

Did you ever feel like losing control over your personal data?

Here comes a new regulation called **General Data Protection Regulation (GDPR)** that is likely to have a far-reaching impact on all major organizations with global operations.

The General Data Protection Regulation (GDPR), proposed by the European Commission (EC), regulates the processing of personal data relating to individuals in the European Union (EU) by any individual, company or organization. GDPR is expected to harmonize all previous data protection regulations throughout the EU comprising 28-member nations, with the prime objective of giving back citizens control of their personal data.

All organizations operating within the EU come under the purview of GDPR by default. Additionally, GDPR is applicable to organizations outside EU offering products and services to customers and businesses in the EU. This implies that GDPR is likely to have a far-reaching impact on all major organizations with global operations.



GDPR came into force on May 24, 2016 replacing EU's Data Protective Directive of 1995 and will be applicable from May 25, 2018. According to EC, GDPR is expected to save EUR 2.3 billion per year across Europe.

The International Association of **Privacy Professionals (IAPP)** predicts that Fortune's Global 500 companies will spend around USD 7.8 billion in order to ensure compliance with GDPR.

According to a recent survey by **PricewaterhouseCoopers (PwC)**, more than 90 percent of US companies consider GDPR a top data protection priority.

Scope of GDPR



All commercial businesses, charities and public authorities in the EU that collect, store or process an individual's personal data come under the ambit of GDPR.

Service providers that process data on behalf of an organization also need to comply with the regulation.

GDPR stipulates that processing of personal data must be in accordance with the standard data protection principles.

These encompass collection of relevant data only for specific legitimate purposes, fair and transparent data processing as per the law, storage only for the essential period, ensuring accurate and up-to-date information in addition to security, integrity and confidentiality.

Types of Data Handlers

The GDPR legislation applies to two different types of data handlers: 'Processors' and 'Controllers'.

According to Article 4 of GDPR, a controller is a "person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data", while a processor is a "person, public authority, agency or other body which processes personal data on behalf of the controller".

The data controller not only defines how personal data is processed but also ensures that both internal resources and external contractors comply with the regulation. Data processors can comprise either internal groups or any outsourcing firms that are involved in processing and maintaining the personal data records.

GDPR Breach Notification

Risk fines of up to
€20 million
 or 4% of your organisations
 global turnover



All organizations under the purview of GDPR must report instances of data breaches involving unauthorized access or loss of personal data to the supervisory authorities and also inform individuals impacted by the breach.

Any breaches likely to lead to financial loss, loss of confidentiality or damage to reputation must be reported within 72 hours without fail. Non-compliance by organizations could lead to fines of up to **4% of the global turnover or EUR 20 million**, whichever is higher.

Types of Privacy Data Protected by GDPR

GDPR ensures the protection of personal data such as name, address, email address, photo ID of individuals, along with biometric data, racial or ethnic data, political opinion and sexual orientation among others.

Similarly, web data including IP address, profiling and analytics data, cookie data, location and RFID tags are also protected.

Privacy Guidelines



GDPR enforces data protection measures such as "Privacy by Design" and "Privacy by Default".

'Privacy by Design' requirement ensures that organizations design procedures, policies and systems that are in compliance with GDPR right from the initial stages of the product or process development. It takes into account the context and scope of processing along with the implications.

'Privacy by Default' places an obligation on data controllers to ensure that the personal data collected is utilized only for specified purposes by implementing appropriate measures at the organization level.

While implementing 'Privacy by Design' and 'Privacy by Default' is not a big issue for organizations already possessing a strong privacy policy, they must be adhered to without exception for compliance with GDPR.

Appointment of Data Protection Officers

GDPR mandates that organizations carrying out large-scale processing of certain special categories of data and large-scale monitoring of individuals must appoint a Data Protection Officer (DPO). Public authorities also need to appoint DPOs mandatorily.

The DPO informs and advises an organization regarding its obligations and ensures that the law protecting the personal data of individuals is applied correctly. In addition to strengthening data governance and monitoring compliance with GDPR, the DPO acts as the point of contact in working with the data protection authorities on formulating policies and standards

Individual Rights under GDPR

GDPR enables individuals to have a greater control over their data while reducing the power to organizations that collect and utilize such data for monetary gains.

Individuals can exercise the following rights under GDPR:

1. The right to access: Individuals can request companies for access to their personal data that will be provided to them free of charge.
2. The right to be forgotten: Individuals have the right to have their data deleted by withdrawing their consent to a company's usage of their personal data.
3. The right to data portability: Individuals have the right to transfer their data to another service provider in a commonly-used and machine-readable format.
4. The right to be informed: Companies must inform individuals and take their consent before gathering their personal data.
5. The right to have information corrected: If individuals find their data to be incorrect or incomplete in the company records, they can get it updated.
6. The right to restrict processing: Individuals have the right to stop their data from being processed and used.
7. The right to object: This right, which ensures that data processing for direct marketing is stopped immediately upon request, must be informed by companies to individuals at the very beginning of any communication.
8. The right to be notified: In the event of any breach of personal data, individuals have the right to be informed within 72 hours.

Rules for Obtaining Customer Consent

GDPR compliance requires organizations to clearly specify how personal data of customers will be processed, the reason for processing and also who will process the information. Privacy notices need to be provided in a concise and easily accessible form using simple and plain language.

Customer consent is one of the core tenets of GDPR. Organizations must be able to provide evidence that customer consent has been obtained freely without coercion using only fair means. Pre-ticked boxes or any other methods of default consent must be avoided.

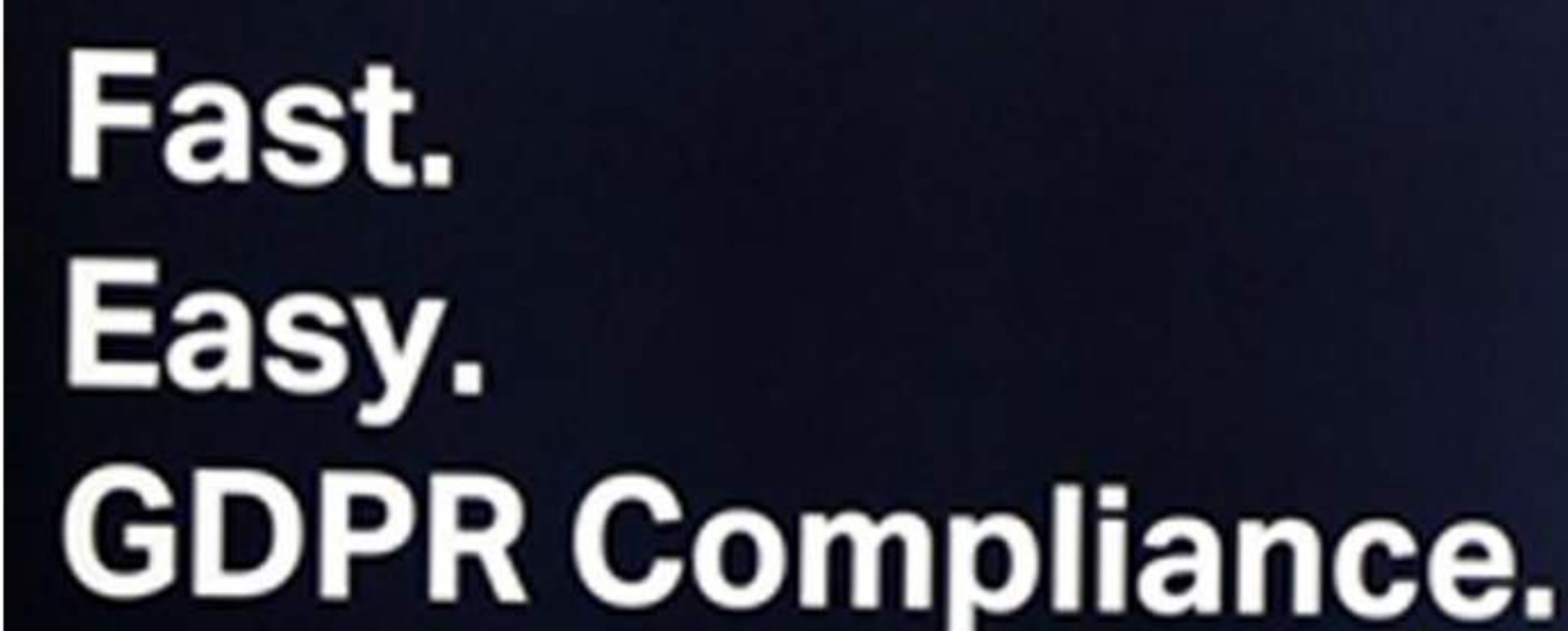
Parental consent is mandatory for utilizing the data of children under the age of 16. However, member states can authorize a lower cutoff limit for parental consent, as long as it is not lower than 13 years.

Genuine customer consent not only leads to building customer trust and engagement but also contributes to enhancement of organizational reputation.

Benefits of GDPR Compliance

GDPR provides organizations with opportunities to make their business more secure, efficient and competitive. Some of the tangible benefits of GDPR compliance include:

- **Increased Cybersecurity:** GDPR drives companies towards reevaluating and improving their overall cybersecurity strategy in addition to building stronger data protection workflows and streamlining security monitoring.
- **Enhanced Data Management:** Data auditing, a prime requirement for GDPR compliance, helps organizations in minimizing the data they collect and hold, and refining the data management processes.
- **Improved ROI on Marketing:** GDPR ensures that organizations receive a database of only relevant leads and customers who are genuinely interested in their brand. This results in higher click-through, conversion rates and increased marketing ROI.
- **Gaining Customer Trust and Loyalty:** GDPR requires companies to be highly transparent in the way consumer data is gathered and handled, resulting in increased trust and loyalty from both current and prospective customers.
- **New Business Culture:** Adherence to GDPR introduces a new employee mindset that includes respect for customer data privacy and helps in nurturing a social responsibility that is focused on data security.



**Fast.
Easy.
GDPR Compliance.**

Preparing for GDPR Readiness

Organizations must evaluate their data handling mechanism and incorporate the necessary steps for ensuring compliance with GDPR. The path to GDPR compliance includes a few challenges that need to be addressed such as:



- **Stakeholder Involvement:** An organization's IT department is alone not responsible for meeting the GDPR requirements. It is essential to form a task force comprising personnel from various departments such as marketing, sales, operations and finance that collect and make use of customers' personal information. This task force can implement the procedural and technical changes required for GDPR compliance.
- **Risk Assessment:** A comprehensive risk assessment must be undertaken along with implementation of measures to mitigate any possible risks.
- **Data Storage and Access:** All the departments in an organization must clearly identify where the personal data is stored and who all have access to it.
- **Team Compliance and Training:** All teams must be trained and made aware of which information can be divulged and what constitutes noncompliance.
- **Data Protection Plan:** Companies need to create a data protection plan and periodically review and update it to ensure that it is in alignment with GDPR requirements.

In Conclusion

GDPR represents a paradigm shift in the approach towards the handling, processing and securing of personal data.

The downside of GDPR is that while the regulation protects citizens from non-European countries who live in the EU, it offers no protection to EU citizens living and working outside the jurisdiction of EU.

United Kingdom will have to comply with the GDPR rules at least until the nation's exit from EU towards the end of March 2019, though the implications of GDPR on a post-Brexit UK are still unclear.

Most IT leaders believe that compliance with GDPR requirements will provide their organizations with a tremendous competitive advantage in addition to boosting their efficiency in data management. This in turn will lead to enhanced customer confidence and satisfaction in the long run.



info@veritis.com



1-877-VERITIS (283-7484)



972-753-0033



US Corporate Headquarters

1300 W. Walnut Hill Lane
Suite 190
Irving TX 75038



India Headquarters

#607, 6th Floor,
Ashoka Bhoopal Chambers,
S P Road, Begumpet
Hyderabad - 500003, India.
Phone no: 040 42211730



Development and Operations

1231 Greenway Drive
Suite 1040
Irving, TX 75038

For more information, contact info@veritis.com

© Copyright 2018 Veritis Group, Inc. All rights reserved. Veritis Group, the Veritis Group logo, and other Veritis Group marks are trademarks and /or registered trademarks of Veritis Group, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

veritis.com