How does GDPR Regulation help in Data Protection and Data Privacy?

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

General Data Protection Regulation Act is a popular and widely accepted EU law that is concerned with the data protection and privacy of citizens of the EU. It is said to be the most stringent data security and privacy law enforced by the EU enforcement directives. Organizations that are subjected to the Regulation need to understand the significance of the two broad categories of compliance, namely Data Protection and Data Privacy for its successful implementation. Today's article covers details on how the GDPR Regulation facilitates data protection and data privacy of citizens of the EU. The article will briefly shed a light on the regulation and explain how Data Protection and Data Privacy are interrelated.

Data Protection and Data Privacy: How are they different yet inter-related

More than often, organizations believe that by securing their sensitive data they are also covered for the data privacy regulation. But, that is not the case. Data Security and Data Privacy is often interchangeably used and has often led to the ignorance of implementing necessary measures to cover both the essential aspects of the Regulation. It is critical that your business understands the difference and addresses the two individually or it will have a significant impact on your business. Data Privacy is a part of the broader spectrum of Data Protection which is concerned with secure processing, storing, and management of sensitive data. So, while data protection ensures securing of data from unauthorized access, data privacy is about empowering individuals of their privacy rights. So, while Data Security protects sensitive data against external attackers and malicious insiders, the Data Privacy governs how the data is collected, shared, and used considering the individual's consent for the same. The below-given table will precisely outline the differences between Data Privacy and Data Security.

Data Security VS Data Privacy

Data Security	Data Privacy
Data security focuses on protecting sensitive data against unauthorized access and use.	Data Privacy focuses on ensuring appropriate handling processing, storage, and use of Personal Information and defines who has the authorized access permission
It is more about protecting the integrity of the data and ensuring data accuracy, reliability, and availability to authorized parties	It is about the rights of individuals with respect to their personal information.
Data security is for any kind of sensitive data be it personal, financial, or any confidential information.	Data privacy is more about securing the personal information of an individual.
Data security is the responsibility of the organizations handling and using the data.	The control of data privacy is in the hands of individuals who can decide on how their data can be used or shared
Data protection aims at securing information from hackers.	Data privacy aims at securing the data from being shared or sold without the individual's consent.
Data protection is a mechanism to secure sensitive data against hack or theft.	Data Privacy is a regulation comprising of policies and procedures that helps govern the data.
Data security may not necessarily include data privacy	Data security may not necessarily include data privacy

Basically, Data protection is nothing but an amalgamation of security measures and privacy policies. Now that we have covered the key differences between Data Security and Data privacy, let us move on to understand the GDPR Regulation and learn how it helps in data protection and data privacy

GDPR Regulation

General Data Protection Regulation Act is a law that aims at securing the data and privacy of citizens of the EU. It is a Privacy law that has a direct impact on businesses around the world dealing with sensitive data of EU citizens. GDPR mandates standards for companies that handle EU citizens' data to safeguard the processing and movement of citizens' personal data. The regulation clearly outlines certain requirements pertaining to data protection and data privacy for organizations to follow. All organizations falling in the ambit of the regulation be it, small businesses to large enterprises, must be aware of all the data privacy and security requirements of GDPR and accordingly comply with it. Moving ahead, let us now understand what the GDPR says about Data Security and Data Privacy.

GDPR Regulation on Data Protection

If your organization falls under the ambit of GDPR Regulation your organization is expected to meet the requirements as stated in the protections and accountability principles outlined in Article 5-6:

Lawfulness, fairness, and transparency- The requirements outlined in the GDPR Regulation clearly states that the processing of data must be done fairly, lawfully, and with complete transparency.

Purpose limitation- The article also clearly states that the organization must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

Data minimization- Organizations are expected to collect and process only as much data as absolutely necessary for the purposes as specified.

Accuracy of Data- As per the stated requirements, organizations are expected to keep personal data accurate and up to date.

Data storage limitation — Organizations are allowed to store personal data for only as long as necessary for the specified purpose.

Integrity and Confidentiality of Data- The data collected must be processed in a way that ensures appropriate security, integrity, and confidentiality of information. This can be achieved by adopting the technique of encryption.

Accountability- The data controller is responsible for demonstrating compliance with all of the standard requirements set in the GDPR Regulation.

GDPR Regulation on Data Protection

The GDPR Regulation also lays out Data Privacy rights and principles for organizations to follow when processing the personal information of citizens of the EU. Articles 12-23 in Chapter 3 clearly draws out principles that the organizations are obliged to facilitate data subject rights.

Right to Transparency in information, and communication for exercising data subject rights-

Organizations are expected to communicate in a concise, transparent, intelligible, and easily accessible form, using clear and plain language on how the data is processed. Further, organizations are expected to inform and make it easy for people to make access requests, rectify, erase or restrict the processing of data. Organizations are expected to respond to those requests quickly and adequately.

Right to be informed- Data Subjects have the right to be informed about where their personal data is collected from, how they are processed, and to whom they are shared.

Right to access- Data subjects have the right to access information pertaining to their personal data from the controller. The type of information that can be accessed may include the category of personal data, the purpose of processing data, source of collected data, location of storing data, or duration of storing data to name a few.

Right to rectification- Data subject has the right to demand rectification of inaccurate information of their personal data without any undue delay.

Right to erasure- Data subject has the right to demand erasure of their personal data without any undue delay. This would include also the right to withdraw their consent of processing data at any point of time considered appropriate by the data subject.

Right to restrict processing of data- The data subject has the right to restrict the processing of data in the pretext of them processing inaccurate information, illegal purpose, or processing beyond the original purpose specified.

Right to data portability- The data subject has the right to receive their personal data in a structured, commonly used, and machine-readable format. They further hold the right to transmit those data to another controller without hindrance from the controller who currently has it.

Right to object- Data subject has the right to object the controller from collecting or processing your personal data. However, the controller can override the objection by providing a legitimatebasis for using the data

Right to notification obligation- Based on the data subject's right to restrict, object, or erasure of their personal data, the controller is obliged to notify and ensure the requests are met by the third-party with whom they have shared the information. Right to object automation of decision- Data subject has the right not to be subjected to an automated decision of processing, including profiling, which have a legal effect on him or her.For more details on the Data security and privacy rights outlined in the GDPR Regulation, you can refer to the link https://gdpr.eu/tag/chapter-3/

Conclusion

Considering the growing concerns of Data Security and Privacy in the industry, the GDPR Regulation was established and enforced across the EU. With its far-reaching implications on businesses globally, organizations are now expected to implement the best practices to ensure Data Security and Privacy of personal information. The purpose of imposing the regulation is to ensure consistency in the data protection and privacy laws across the EU and for organizations globally, if applicable to them. The enforcement of the regulation has surely had a positive impact on the cyber security industry, ensuring the implementation of the industry's best privacy law for securing data.

Original Source:- Cisomag.eccouncil

Written By:- VISTA InfoSec

Do write to us your feedback, comments and queries or, if you have any requirements: info@vistainfosec.com

You can reach us on:

USA +1-415-513 5261 | INDIA +91 73045 57744 | SINGAPORE +65-3129-0397 | UK +447405816761