Role of encryption in GDPR Compliance

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

Encryption has been a hot topic of discussion during the implementation of most Data Privacy laws. In the age where organizations are dealing with large volumes of data each day, the protection of this sensitive data is critical. The data which is seen as a business-critical asset for organizations should be protected against hackers looking for opportunities to steal the data. For these reasons, most Data Privacy Regulations call for organizations to encrypt their data and prevent incidents of cyber-attacks.

Today's article is about one such Data Privacy law that repeatedly mentions about the adoption of the encryption technique. GDPR Regulation is a Data privacy law in the EU that mentions about the use of encryption. Although not mandatory, it is yet seen as a best practice for protecting personal data. So, let us first understand what data encryption is and then understand the role of encryption in GDPR Compliance.

What Is Data Encryption?

Data Encryption is a process or technique of translating data from text to hashed code that can only be decrypted with a special key. This is one of the most effective processes organizations can incorporate to enhance their data security measures.

The purpose of encrypting data is to maintain the confidentiality of sensitive data. Often unencrypted data which is stored in computers, or on servers or transmitted using insecure internet or insecure computer networks can result in incidents of data breaches. Having stored or transmitted unencrypted data can jeopardize the confidentiality of the data and lead to data sprawl and hacking.

Benefits of Data security encryption

Encryption plays a crucial role in the security of data. The encryption algorithms ensure confidentiality, privacy, and integrity of the data. It also ensures authentication, access controls, and non-repudiation of sending data. There are more benefits to incorporating the technique of data encryption. So, given below are some reasons why data should be encrypted.

Data Protection – Data encryption ensures complete protection of data against any kind of hack or threat. The sensitive data cannot be accessed by unauthorized personnel nor can it be stolen in any way.

Secure Data Transmission- Encryption of data also ensures secure storage and transmission of data. So, even if the data is being transmitted through an unsecured network you can still be rest assured of it remaining confidential. Files that are shared or uploaded to the Cloud systems will remain safe throughout the process of transmission.

Data Integrity Maintained- The risk of data alteration is often overlooked in most cases. However, by encrypting data with a digital signature or a checksum, it will be secured against unauthorized alterations of data; even incase the incident happens, it will easily detected. In other words, tampering of data can be identified in case the data is compromised.

Ensure Compliance- Compliance is extremely important for businesses and so they are expected by the law to comply with the industry regulations and standards. Encryption is one of the safest techniques that businesses can adopt to securely transmit and store data and comply with the various Data Privacy and Data Security Standards.
So, what does encryption have to do with the EU's GDPR Data Privacy Regulations? For better understanding let us take a closer look at the GDPR and its requirements.

What does the Regulation say about the GDPR encryption requirement?

General Data Protection Regulation Act is a data privacy law that requires organizations to implement measures to protect the privacy, integrity, and confidentiality of data. Although the regulation does not mandate or explicitly call for data security encryption, yet it requires organizations to enforce the best security measures and safeguards. The Regulation recognizes the risk exposure concerning the processing of personal data and so it places the responsibility on the controller and the processor in Article. 32(1) of GDPR to implement appropriate technical measures to secure personal data.

While the regulation does not specify specific technical and organizational measures to be considered, it yet emphasizes encryption techniques. Despite not being a mandate, the GDPR Regulation repeatedly mentions encryption and pseudonymization as an appropriate technical and organizational measure for GDPR data security. The regulation clearly places the responsibility on the controller or processor to decide where the encryption is required to be implemented.

Encryption of personal data in general offers additional benefits for controllers and/or processors. So, in case there is a misplacement or loss of storage medium which holds personal data that is encrypted, may not be considered as a data breach, provided the incident is reported to the data protection authorities. Again if there is an incident of a data breach, the authorities may take into consideration the use of encryption in their decision on imposing fines as per Article 83(2)(c) of the GDPR.

GDPR Encryption Requirements: Final Thought

GDPR Data encryption can be a highly effective technique for GDPR Compliance. Although GDPR encryption requirements are not mandatory, it is yet a powerful technique for data security. as it converts or encodes information into a non-readable format that only an authorized party can access and read. This way, the GDPR data encryption strategy can work out to be beneficial for your organization especially when it comes to preventing data breaches. So, regardless of whether the GDPR or another regulation applies to your organization, encryption forms an integral part of any organization's GDPR Data security. Either way implementing GDPR data encryption will prevent your organization from being vulnerable to a data breach and costly fines which may cost much more than its implementation cost.

Original Published on:- Tripwire
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