General Data Protection Regulation (GDPR) Compliance
It's Impact on Data Security and Protection Programs

Increasingly, data protection has become an important issue across the globe. In light of the recent high profile series of data breaches, the need to ensure data confidentiality has become ever more important.

With the introduction of the General Data Protection Regulation (GDPR), the European Union (EU) has shifted data protection to a new level. The GDPR legal framework is now in operational and it is scheduled to be enforced starting the 25th of May 2018. Organizations have less than 18 months to ensure compliance and to have the appropriate organizational and technological control measures in place

GDPR plays a significant role for the European Union countries where it is aimed at merging the 28 member's national markets to one market designed for the digital age. Given the nature of data and data collection, in practice, the GDPR is impacts almost every organization worldwide that is involved in either data collection or processing on individuals within the EU. This is inclusive of expatriates, permanent residents, and the visitors.

Contribution towards this priority has been made possible through the regulations that have been set by the organization. Firstly, it modernizes both (taking into account of the fast technological development and its significance over the past two decades) as well as harmonizing data protection legal framework across the EU countries for data protection and discarding minor implementation approaches of the previous directives. The EU commission estimates that businesses can save up to € 2.3 per year with one law for data protection across the 27 states. This ensures that data protection is not made and managed in different markets. Secondly, there is a level playing field now for data protection organizations.

GDPR compliance is, therefore, is upheld on the individual's geographical location and whereby a certain organization holds personal data despite the organizational domicile registration. This overview does not only show how the EU protects their data but also how global data protection should be carried out since serious penalties are charged upon non-compliance to the GDPR policies (Barker et al., 2013)

GDPR Highlights

The GDPR is proving to be a more comprehensive framework way for data protection as compared to the earlier methods. Two key reasons as to why the GDPR is important are highlighted below:

- GDPR should be applied to not only the organizations that are members of the European Union but also to all other organizations because it mandates unique data protections and provisions that processes or controls EU residents' personal data with relation to offering services or goods and monitoring behavior taking place within EU. In conclusion, not being a member of the EU organization does not factor one out from data controller.
- Finally, the organization realizes a financial penalty regime of up to € 20 million which is equal to a 4% annual worldwide turnover of the preceding financial year higher

GDPR Implications

Since there is a massive cost for non-compliance ranging from financial and non-financial terms, ignoring the implementation and response to GDPR are invalid. Three suggested implications that can be considered by decision-makers in regard to GDPR are as below;

i. Personal data re-examination strategy. This implies that every organization should have frameworks geared to data security.

ii. Efforts by the non-EU members to catch up. This means that every organization should put efforts in complying with the GDPR regulation to ensure data security for their clients and their operations. This will ensure avoidance of massive penalties imposed for non-compliance.

iii. Response to both technological and organizational issues. Technology alone insufficient to comply with the GDPR mandate. However, by all means, every organization is expected to comply with the right technological means. Organizations IT departments cannot bear the burden to meet the requirements of the GDPR.

GDPR Requirements

There are a number of requirements that are set by the EU organization aimed at data protection for its residents. These requirements are meant to protect data privacy of people as well as compliance of the GDPR in both technological and organizational measures. Some of them are as highlighted below

i. The ability of compliance demonstration. Organizations ought to demonstrate technological and organizational measures.
ii. Upholding legal basis for any form of processing. Upon processing of any individual data, legal procession should be considered.
iii. When processing various data types, special and different conditions of data categories should be taken into consideration.
iv. Article 30 of the EU requires that a system keep track of all the processing data to be put into operation.
v. Upon data mishandling or breach, notifications should be initiated within 72 hours.
vi. Standard of consent increase.

Data Encryption: Helping Organization Comply with GDPR

Data encryption standard is basically the use of the algorithm for the transformation of stored data into ciphertext that can be first decrypted for comprehension. This method is therefore used for database protection against malicious interventions by individuals. This method of data protection helps in protection of data from the hacking of the aforementioned database whereby encrypted data is of no use by hackers (Barker et al., 2013).

Among the various methods of data encryptions used to retain privacy are: External database encryption, column-level encryption, Field level encryption, Encrypting file systems and symmetric and asymmetric database encryption.

Among other technological requirements for the GDPR compliance, data encrypting is one of them. Encryption as a technology for data protection plays a key role for GDPR and its presence, therefore, mandates its use by the organization. Through encryption, system breach for accessing the data by the unauthorized individuals is minimized. Encryption is designed in such a way that data is protected at rest and while in application use so that data protection can be ensured at any instance when breach may occur. By this doing, therefore, GDPR penalties are reduced. Data encryption within existing database format is enabled by some vendors to protect personal data. This helps in enhancing data protection without necessarily requiring redevelopment of current applications and systems. This style of data encryption enables protection while in use and at rest whereby data protection systems can continue to function normally without the clear use.

Encryption Risks

Despite the database encryption advantages for data protection, it is imperative to consider and be aware of the risks involved in the process. One of the encryption shortcomings relates to the data management. Failure to manage private keys in an "isolated system", malicious system administrators may be able to decrypt the data and access sensitive data. Secondly, loss of fundamental principle of keys may lead to a devastating risk which leads to data not being decrypted and eventual loss of essential data (Basharat, 2012).

ParaDoxBox™

As part of an overall data security program, SCI's **ParaDoxBox™** rapidly enables organizations to achieve GDPR compliance. **ParaDoxBox™** protects information on computers, network storage, and the Cloud. Incorporating an advanced patented encryption process, biometrics, and location-based authentication technology, ParaDoxBox™ offers enhanced security that protects sensitive information. It protects data on endpoints, network storage and Cloud locations. Incorporating superencipherment, Idiomatic Recognition™ and location based authentication technology, ParaDoxBox™ offers enhanced security that is compliant with FIPS 140-2, HIPAA, HITECH, and CJIS.

- No training burden; no change to human-machine interface
- Users choose storage locations and algorithms that encrypt data
- Protects device, network and Cloud storage locations
- Incorporates advanced superencipherment and multifactor authentication

About Secure Channels

www.securechanels.com

Secure Channels is an Orange County, California based authentication and encryption company.

Sources

Barker, W. C., & Barker, E. B. (2013). SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.

Basharat, I. (2012). Database security and encryption: A survey study. *International Journal of Computer Applications*, *42*(34).

Koops, B. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. *International Review of Law, Computers & Technology*, *58*(5), 129-133.

