LTIMindtree

Point of View

Key GDPR Challenges – Fix the House

Top 10 Questions to Answer

Author

Manoj Shikarkhane

EVP and Global Head – Software Engineering Group

The Importance and Relevance of the GDPR

Data is one of the key assets of an organization. With big data, analytics and artificial intelligence, data has given organizations significant competitive advantage. However, data protection and data privacy have been compromised by practices and processes that have not been stringent and rigid. With the introduction of the revolutionary European General Data Protection Regulation (GDPR), data driven organizations face the risk of steep penalties in case of non-compliance and data breaches.

With the enforcement of the GDPR just under a year away, organisations are preparing for its far-reaching implications. Effective from May 25, 2018, the regulation is likely to impact over 150 countries, which deal with the EU resident data.

What makes the GDPR different from the existing data protection regulations is the significant new obligations that the data processors and the controllers need to comply with. Also, the GDPR extends the law to organizations/entities dealing with people residing in the European Union, regardless of their geographical location. The tenets of responsibility, accountability and liability have changed to make organizations responsible for implementing data protection policies in their business.

Key Challenges in the GDPR Implementation

While the GDPR mandates hiring a DPO, in some cases finding the right talent either within the organisation or outside will be challenging. Given the mandated responsibilities of the DPO, the person hired for the role will need to be senior and experienced. This also puts additional financial burden on a company. However, a well-qualified DPO will also help organizations save potential fines and other risks.

Organisations will be required to collect and retain only as much data as is necessary for a specific purpose. Identifying the right amount and type of data is critical. Hence, it is imperative for organizations to properly document the source of data, its storage as well as whom the data is being shared with.

The GDPR is essentially about explicit consent from customers. Organisations will need consent from customers before using their personal data for marketing and sales strategies. It also mandates that the language in which the consent is sought is simple, precise and easy to understand for anyone.

The penalties for non-compliance are significant and can put a dent in an organisation's revenues. 4% of the revenues are a significant amount. As high as the financial risk is, organizations will also have to deal with reputational and geographic risks since this is an EU wide regulation.

TOP 10 QUESTIONS **TO ANSWER**
for the GDPR Implementation

Question 1 – How to ensure successful adherence to the requirements of GDPR?

The key is to ensure that data protection is woven into the business processes. Reviewing all the data held by the organisation and understanding the silos is critical. This needs to be enabled across the organisation and not just the IT departments.

Question 2 - How can the organisation educate its employees?

With heightened scrutiny in the implementation of GDPR, it has become necessary for organisations to have frequent training and orientation programmes in place. For instance, it's critical to explain to people how to make notes and record data regarding their customers, prospects and employees. It may seem rather rudimentary and obvious but this data could be subject to a data access request.

Question 3 – Does this mean we need new technology?

Since the GDPR requires organisations to be much more vigilant in ensuring that personal data is suitably protected and only available to individuals with the appropriate consent and authority, investment in technology is imperative. Encryption, analytics, perimeter security, and consent management are only some of the things that will need investments. This also means working with an IT infrastructure partner who understands your business and the criticality of your data, considering the GDPR requirements. Robust infrastructure to ensure adequate collection, storage and processing of data is essential for the GDPR along with a mechanism to regularly review and update the infrastructure.

Question 4 – What is the risk of non-compliance?

The GDPR holds the data controllers and processors severely accountable for non-compliance. Apart from the monetary risk, there is also a reputational risk since the regulation is enforced across the European Union.

Question 5 - What is the extent of personal data an organisation can have?

Organisations have access to and collect far more information than is required. The GDPR raises the issue of the amount of personal data an organisation can collect and retain. Reducing the amount of data collected would be a simpler solution to reduce costs. The more the amount of data, the higher the need for encryption, thus making more investments inevitable.

Question 6 – Does this mean that the entire business orientation needs to change?

While the GDPR requires organisations to critically examine their business processes, data protection and privacy now become strategic to organisations. It can also be viewed as an opportunity for a larger digital transformation in the organisation to enhance transparency and strengthen customer experience.

Question 7 - How can the organisation minimise risks and protect its reputation?

There are several ways an organisation can do this. Firstly, documenting the type of personal data needed by the organisation along with its source and who it's shared with is critical. Secondly, develop a roadmap to determine your sources for data input, data processing tools, techniques, and methodologies that you use, and how the data you hold is shared with other businesses. And last but not the least, customers' requests of consent withdrawal must be dealt with in an efficient manner and updated in the system to flag that the user has withdrawn consent to prevent further use of his/her personal data.

Question 8 – How does the organisation ensure consent from customers?

Under the GDPR, individuals have to explicitly consent to the acquisition and processing of their data. Vaguely acquired consent in the form of checking boxes or implied consent may not be acceptable anymore. Organizations will need to thoroughly review their privacy and data disclosure statements. Language for consent also needs to be clear and precise.

Question 9 – How does the organisation ensure the enhanced security measures?

Organisations must develop and implement safeguards throughout their infrastructure to help contain any data breaches. This means putting security measures in place to guard against data breaches, and taking quick action to notify individuals and authorities in the event a breach does occur. Engaging with a partner that can help the organisation manage these security measures will help in ensuring compliance.

Question 10 – Should all organisations appoint a Data Protection Officer (DPO)?

The GDPR requires only public authorities, organizations with data processing operations or those processing large amounts of personal data to appoint a Data Protection Officer. An individual with a reasonable understanding of the organization's technical and organisational structure and familiarity with its IT infrastructure and technology can qualify as a DPO. While it may not be mandatory for all organizations to have a DPO, it would be prudent to have an individual or team supervise the compliance processes.

Conclusion

Compliance with the GDPR requirements may seem daunting given the countless permutations of compliance issues. However, underestimating the impact can also be detrimental to organisations, making them susceptible to vulnerabilities that come with the highly sensitive nature of this law. There may be some uncertainty as to how to prepare for this change, but it's clear that the law requires streamlining and structuring of processes with regards to data. While the journey towards compliance can involve substantial costs and efforts, the upside involves improved customer value as well as brand equity.

LTIMindtree's end-to-end GDPR framework can help you to assess the GDPR impact on your business, help put in any necessary changes, allow breach monitoring and recovery, and provide security assurance to simplify the complexities of the GDPR.

About the Author

Manoj Shikarkhane

EVP and Global Head – Software Engineering Group

Manoj is specialized in the development of custom built applications. Has 29 years of experience in managing offshore dedicated centers for customers across the sectors in the globe. He has managed transformational projects in application development and testing space. Manoj's current focus is to transform traditional software engineering practices leveraging cloud ecosystem.

LTIMindtree