LTI

Let's Solve

Compliance no longer an After-Thought:

What it takes to be GDPR-Ready?

Author

Soumendra Mohanty

EVP and Global Head – Cognitive & Analytics

July 2017

A Larsen & Toubro Group Company

The General Data Protection Regulation, or GDPR, was adopted by the European Parliament in April 2016, and it introduces obligations for data controllers and processors in several areas: strengthening the rules for obtaining consent, strengthening the need for breach notifications and strengthening self-assessment in the management of data. These rules apply to both, the EU member states, and to organizations outside the Union when processing the data of citizens within it.

These sweeping changes have made the GDPR implementation and preparedness not just another compliance program, but a comprehensive privacy protection and data management program, by design and by default. It is a program that entails embedding data protection and data management requirements throughout the organization at every stage of each business process, from inception to operations. Why so?

Data is critical to many business processes, products and services. The digital economy is primarily built upon the collection and exchange of data, including large amounts of personal data, much of which is sensitive in nature. Personal data in the GDPR context has a broader purview. It refers to any information relating to a person who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, online identifier; or by one or more factors specific to the physical, physiological, genetic, mental, racial, socio-economic, cultural or social identity of that person. These expanded purview of personal data mean that online identifiers, including the IP address, cookies, and so forth, will now be regarded as personal data if they can, without undue effort, be linked back to the data subject.

The implications are far reaching, especially for the digital economy, where things such as recommendation engines, next best offers, hyper-personalization and social media data analysis to arrive at micro-segmentations of customers, need to be re-imagined due to lack of distinction between personal data of individuals in their private, public or work roles – after all, a person is a person. Personalization and other targeted marketing techniques, rely on a degree of selection, which is typically built on profiles of demographics, behaviors, purchases, socio-economic parameters and location awareness. With powerful big data analytics platforms and sophisticated machine learning algorithms, many of these profiling activities and the subsequent targeted marketing campaigns are increasingly becoming automated. The regulation specifically highlights that individuals have rights not to be subjected to the results of automated decision-making, including profiling, and they can opt out at any point in time.

In other words, it needs to be obvious to the data subjects what their data is going to be used for at the point of data collection. Organizations need to be able to show clearly how consent was gained, when it was gained and for what purpose. And at the same time, withdrawing consent should always be made possible and should be as easy as giving it. This aspect of the regulation has extensive implications not only on the business processes and the applications at an enterprise level, but also for the core data management areas. Organizations will need sophisticated lineage and traceability methods to track

personally identifiable data of data subjects across the business process landscape, and they would also need a seamless purge method to soft or hard delete the personally identifiable data if the data subject wishes to exercise an opt-out option.

The regulation mandates controllers and processors to implement appropriate technical and organizational measures, including anonymity and/or encryption of personal data. Organizations will have to think harder about privacy, and implement a risk-based approach where appropriate controls must be developed according to the degree of risk associated with the data processing activities. An increased emphasis on data lineage and traceability is critical to help demonstrate and meet compliance, and also improve the capabilities of organization to manage privacy and data effectively.

GDPR puts greater emphasis on data security. The GDPR requirements state that businesses will have to notify the data protection authority if there is a security incident that affects the integrity, confidentiality or security of the personal data that they hold. If the breach is likely to result in discrimination, identity theft or fraud, financial loss, damage to reputation, or other significant economic or social disadvantages for data subjects, businesses will have to notify the breach to the affected data subject.

Importantly, no notification to the data subjects will be required if businesses have implemented appropriate technical and organizational security measures with respect to the data affected by the breach. So if, prior to the breach taking place, the data were rendered unintelligible, for example, by means of an encryption, businesses will not have to notify the data subjects of the breach.

In the event of a personal data breach, data controllers must notify the appropriate supervisory authority not later than 72 hours after having become aware of it. If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay. Should the controller determine that the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, it must also communicate information regarding the personal data breach to the affected data subjects. This means, organizations must implement processes, tools and technologies to continuously monitor their systems, data, as well as all the access points.

This is why GDPR implementation must be a concerted effort across the organization, with the DPO (Data Protection Officer) working hand-in-hand with Chief Data Officer (CDO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), and other senior leadership.

Getting Prepared

Implementation of such a transformative regulation represents a major challenge for organizations. It is advisable to start outlining a framework and practicing the process as soon as possible, as it will take time to iron out any issue, and perfect it. Moreover, it is an extremely effective way to identify risks to the rights of the concerned people, so that potential flaws in the data processing systems can be methodically resolved. LTI has developed an approach through which we help organizations become GDPR compliant. LTI GDPR domain consultants help organizations assess their readiness for this

change, fix the gaps by implementing the right technology and data solutions, provide insights to the Data Protection Group through metrics and threshold monitoring, and assure compliance for the implementation across Software Development Lifecycle. These key offerings are supported by three main functions – Governance, Change Management and Consulting Services tailored to uniquely meets your organizational needs.

LTI's GDPR offerings simplify the GDPR mandates down to focused modules, each module further delving deep into the specific objectives of GDPR requirements through processes, frameworks, accelerators, tools and services. Implications of GDPR may appear overwhelming, but this regulation represents an opportunity for organizations to consider data privacy compliance more strategically and holistically, as it becomes the key to an organization's data strategy and the digital transformation of its business.

About the Author

Soumendra Mohanty

Soumendra is an acclaimed thought leader and SME in Analytics, IoT, AI Cognitive and Automation space. His expertise is in the Big Data Solutions, BI Architectures, Enterprise Data Warehouse, Customer Insight Solutions and Industry-specific advanced analytics solutions. With over 20 years of Industry experience, Soumendra has designed and implemented data analytics solutions for Fortune 500 clients across Industry verticals.

LTI
Let's Solve

Compliance no longer an After-Thought:
What it takes to be GDPR-Ready?

info@Lntinfotech.com

A Larsen & Toubro Group Company