LTIMindtree

Point of View

Approach to Sustainable **GDPR Compliance**

Author
Swati Koul
Lead- GDPR Compliance Program, LTIMindtree

Approach to Sustainable GDPR Compliance

The General Data Protection Regulation (GDPR) came into effect on May 25, 2018, two years after the regulation entered into force. One of the reasons why enterprises are grappling with finding and fixing the gaps to become GDPR compliant, is the initial wait-and-see approach. While the European Commission gave two years of transition time to prepare for the GDPR, a lot of enterprises spent that time and the corresponding effort sizing up what the law entails, leaving little room for the actual implementation. As a result, most of these enterprises today are focused only on high priority business areas and the risk functions aligned with them. Consequently, they have resorted to manual processes and temporary controls to ensure basic compliance until more permanent IT solutions are implemented in the years to come.

Additionally, broader challenges such as continuous impact assessment reports, breach monitoring and notifications, subject rights & consent tracking, processing of special categories of personal data, etc. are on the verge of becoming an operational nightmare for enterprises, if not tackled right now. Furthermore, as more enterprises adopt makeshift solutions without thorough inspection, the only way to develop sustainable solutions in the long term is to build-in assurance as a part of the CI/CD processes.

Let's look at the most important operational changes that accompany the herculean law.

1 **Privacy by Design and Privacy by Default** – "Privacy by Design" requires to consider privacy throughout the development of new products, services, and processes starting with the initial design stages. "Privacy by Default" calls to establish the most privacy-friendly settings as the default ones when new products, services, and processes include choices on how much personal data individuals share with others. To ensure that privacy is a core ingredient and not just an afterthought in the development process, enterprises will need to develop a comprehensive privacy strategy. This strategy will need to be adopted at an enterprise level and monitored throughout its lifetime.

2 **Beyond Data Security** – Just like embedding privacy at a later stage can be technologically challenging and expensive, implementing IT controls that only secure data can be equally detrimental. Enterprises will need to adopt best practices in areas such as encryption, data pseudonymization or anonymization, and identity and access management. Additionally, they will need to place prescriptive measures at every level – data, application, network, OS & host, cloud, physical, etc. to orchestrate security for better prevention.

3 **Health Monitoring Scans** – The GDPR compliance isn't a one-time activity. Enterprises need to invest in staying aligned with up-to-date assessments of security gaps, as well as any change in the way personal data is being handled internally. These assessments need to act as a periodic check to ensure that the privacy measures adopted are working as expected. The scans also need to be equipped to demonstrate an enterprise's rationale behind certain decisions at a later stage. For instance, to explain why the HR or Payroll systems require stricter controls when compared with a system containing archived information.

4 **Rights Management** – One of the most nerve-racking aspects of the GDPR compliance is to address the data subject rights in a way that doesn't become a massive operational overhead for enterprises. This is more challenging in case of unstructured data in user-defined applications, which tend to take a backseat in the first wave of implementation. So far, manual processes and temporary workarounds have been prevalent, but enterprises will need to take a more pragmatic approach given that the law gives one-month SLA to address a request which can be extended up to two months depending on the complexity and the number of requests.

5 **Insights** – A unified view of the key governance areas, along with timely reporting capability, has become critical. Whether enterprises be decentralized or not, they are likely to experience a sharp rise in compulsory conversations with the supervisory authorities. To cope, they will require automated responsive dashboards which give one-view of the compliance related activities at a master level for quick access and actions. Additionally, mechanisms to better understand user behavior, point to the parts of the websites people have visited, and facilitate and measure the effectiveness of advertisements and web searches, will also need to be developed.

6 **Breach Assist** – The essence of the GDPR aims at breach prevention & neutralization, thus making it along with breach response, and monitoring one of the most important objectives every enterprise needs to work toward. The breach indicators should encompass real-time threat hunting across endpoints, users, IPs, and machines and cater to critical business events through passive scans of threat vectors. They should provide among other statistics, the behavior of breaches, including but not limited to the breach-prone countries, types of breaches observed, techniques to survive the said breaches, etc. Security operations should be driven by cyber analytics that are both prescriptive and predictive in nature.

7 **Assurance** – The ability to manually test and certify 360-degree compliance with the GDPR can be an all-consuming task. To confidently state that an enterprise is ready for the GDPR demands will require thorough testing of the controls, enabling mechanisms for segregation of duties, automating checks, provisioning of an instant alert mechanism for breaches, etc. Whether you are testing for the

rights of the EU residents or validating the effectiveness of security controls through regular vulnerability assessments to ensure Privacy by Design and Default, Assurance is one of the most crucial aspect of the law. Enterprises will need to introduce their products, services, and processes in a controlled manner, only after meticulous and detailed testing.

8 **Change Management & On-going Trainings** – The GDPR is about driving a culture change that transforms with the way users interact, express, and engage in the change journey. Operational metrics such as acceptance ratios and change adoption scores will contribute to the development of culture, and people risk assessments. As digital communication solutions transform the way information is percolated and received by the impacted stakeholder groups, enterprises will need to use the power of these metrics and innovative solutions to design communication that is very specific to the needs and context of their workforce.

Digital boom has led to an over-the-top need of recommendation engines, next best offers, hyper-personalization, and social media data analysis to arrive at micro-segmentations of customers for every enterprise. This calls to develop solutions that can differentiate between personal data of individuals in private, public, or work roles. Moreover, data capture, data mining, data analysis, etc. are no longer intimidating – today they provide vital insights into consumer behavior. They are being used as instruments to create focused campaigns / advertisements to target their customers in new ways.

The GDPR is significant in that it covers every processing operation that can be done on personal data, irrespective of whether it is undertaken by automated or non-automated means, or whether done actively or passively. It requires enterprises to optimize their data-handling processes from both a business, and an end-user perspective. They need a robust plan to handle the influx of GDPR operations in the not-so-far future. It is a tall claim that enterprises can safeguard themselves against the massive operational deluge. However, by focusing on the aforesaid points, they can be well-prepared for when it comes.

About the Author

Swati Koul

Lead- GDPR Compliance Program, LTIMindtree

In her 9 years of experience, Swati Koul has led and delivered large scale cross-functional projects across sectors such as Manufacturing, Media & Entertainment, Consumer Goods, and Banking for Fortune 500 clients. Her areas of expertise include Business Development, Project & Portfolio Management, and Technical Consulting. In her current role, Swati leads the GDPR Compliance Program at LTIMindtree, where she has been responsible for developing the endways service portfolio, which has been positioned in the Leaders quadrant of many analyst reports.