GDPR Compliance: An Action Plan for Financial Institutions

Abstract

The General Data Protection Regulation (GDPR), published by the European Union (EU), has emerged as the torch bearer among the data protection laws. The regulation will have far-reaching impact as it mandates compliance for all organizations that hold or process EU residents’ data. Even if GDPR is not adopted globally, it will form the basis of national data privacy laws. Moreover, it will become a source of competitive differentiation as customers and employees become aware of their data rights and look to engage with organizations that ensure data privacy. This paper takes a look at the impact of GDPR on financial services institutions and suggests an approach to compliance.
Ushering in a New Era in Data Privacy

Consumers leave behind digital footprints whenever they digitally consume products and services. These digital footprints can be processed and analyzed to reveal a variety of private information leaving consumers open to cyberattacks or fraud. Ensuring data privacy has therefore emerged as a key imperative underscoring the need for stronger individual privacy protection mechanisms. The General Data Protection Regulation (GDPR), which came into effect in May 2018, is an effort in this direction. Enterprises established in the EU as well as those that collect and process personal data of EU residents will be subject to GDPR with non-compliance resulting in stringent penalties and reputational damage.

The GDPR provisions will considerably impact the financial services industry given that banks hold enormous amounts of customer data. With high volumes of transactions across numerous channels, multiplicity of processes, legacy systems, and operations across geographies, ensuring GDPR compliance will impact banks’ data management function. Though banks are considered secure custodians of customer data, the focus has now shifted to ensuring transparency in data usage. For instance, a typical customer journey starts with opening a bank account followed by a loan or credit card application. GDPR brings into focus aspects like:

- What happens to customers’ personal data post loan acceptance or rejection?
- Is this data leveraged for cross-selling or up-selling of other financial products? Is consent taken?
- Is the data shared with third parties?
- Post repayment of loan, till when will the customer data be stored on the bank’s systems?

In the above example, under GDPR, banks will need to determine how the personal data stored in loan management systems is processed, consumed, and shared with other systems. Banks will also need to ensure that the data security mechanism adopted for the transfer of data meets GDPR provisions. Furthermore, banks will need to obtain the customer’s consent to use data and make sure that the customer clearly understands what he or she is consenting to.

Banks heavily rely on customer trust and their reputation to retain market position. A violation of privacy laws will leave
banks open to lawsuits and consequent reputation damage – compliance therefore is not only mandatory but also in banks’ competitive interest. Let’s examine some of the key dimensions of GDPR impact on financial services.

**Consent**

Banks must adapt to the enhanced consent requirements by establishing a robust mechanism to secure and store customer consent. The mechanism must enable the efficient management of customer preferences on data processing and change in consent settings with inbuilt review processes to ensure continued compliance.

**Data retention and erasure**

Banks must upgrade existing procedures or adopt new ones to handle the enhanced rights of individuals with regard to erasure, access, correction, and so on. In addition, a clear data retention policy based on business needs must be defined. Data lineage and erasure processes and the associated technology must be in place to enable tracking and deletion of data as and when requested by customers. Similarly, a clearly defined policy on data portability is a must to account for instances when customers request for porting their data to other organizations.

**Privacy by design**

Banks interact with third-party vendors for various operations spanning credit and debit cards, transaction processing at point of sale (PoS) terminals and e-commerce sites, as well as offshore service providers for customer and tech support. Banks need to adopt data masking techniques like anonymization, pseudonymization, and encryption before sharing customer data with third parties to ensure GDPR compliance. Before onboarding new systems, technologies, or vendors, banks must identify privacy risks so that mechanisms to protect data through effective access management can be built in right at the design phase.

**Achieving GDPR Compliance: From Theory to Action**

Most organizations would have put in place processes to ensure a minimal degree of data privacy and adherence with the earlier regulation like the EU data protection directive 1995. However, as GDPR is a more comprehensive regulation, existing processes and the associated documentation may need to be revamped. To achieve compliance, we believe that
organizations must consider the following basic pillars of data protection during the strategy definition phase:

**Executive sponsorship and representation at the C-level**

Successful GDPR compliance will need a buy-in from the top management. Executive sponsorship and stakeholder alignment are crucial as these programs are typically multi-disciplinary in nature, which means that resources must be made available on demand, and roadblocks, if any, must be cleared at the earliest. In addition, to ensure that data is given strategic importance, and GDPR compliance gets the required push from the top, organizations must appoint a Chief Data Officer (CDO) – something that has already started to happen.

**The right compliance strategy**

To enable GDPR compliance, organizations must consult their in-house legal department or external law firms to understand what the law means for the organization and its impact on operations. The next step is to choose the right approach - business process-oriented or system-oriented, or a combination of both, based on a clear understanding of how GDPR compliance is going to affect the prevailing data collection, processing, and deletion mechanisms. While the business process-oriented approach examines how data is collected and processed across an enterprise, the system-oriented approach looks at how data is used and managed by IT systems, and how GDPR will impact such systems.

**Business process-oriented approach:** Organizations must maintain a central repository to record business processes and store the related documentation like business process and underlying data flow diagrams, and details of system interactions. All the business processes across channels and systems must be stored in the central repository, and changes, if any, must be updated – policies and procedures will need to be laid down to ensure that the repository is maintained up to date.

**System-oriented approach:** Given that IT systems are the backbone of business operations, organizations must build a database of systems that process data, the details of the kind of data collected, stored, processed, deleted, and so on, and the existing data management and security policies and mechanisms. A thorough review of existing systems and processes around data management and security must be
undertaken in the light of GDPR to identify gaps. Subsequently, modifications and upgrades must be implemented to address the gaps based on the current maturity and the target state to be achieved.

**Data governance**

Organizations must establish a centralized data governance structure that ensures accountability in the management of core information assets across the lifecycle from definition, creation, security, and usage of data. Due importance must be given to attributes like accessibility, availability, quality, consistency, security, and auditability while designing the governance structure. A centralized data governance structure that covers all the processes, policies, and procedures, clearly defines roles and responsibilities, ensures auditability, and includes comprehensive documentation will go a long way in breaking silos and driving compliance. Data retention and deletion policies, consent management policies, procedures to ensure data subjects’ rights are complied with, and the requisite audit controls must form a part of the governance program.

**People and change management**

People are key to the success of GDPR implementation. Organizations must train employees to ensure a clear understanding of the core concepts of GDPR and the changes it will entail in the current way of working. Employees must also be educated on the consequences of non-compliance, which could range from stringent financial penalties to reputation loss and possible loss of market share.

**The Way Forward**

GDPR is a comprehensive regulation, and it would be easy to get overwhelmed by its reach and complexity. That said, the basic pillars of data protection remain the same. Organizations must define a strategy centred on the core data protection pillars and ensure that they are strong enough to handle emerging scenarios where compliance could pose challenges.
About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Contact

Visit the Banking & Financial Services page on www.tcs.com
Email: bfs.marketing@tcs.com
Blog: Drive Governance

Subscribe to TCS White Papers
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About The Author

Varun Arora
Varun Arora is a Business Consultant with TCS’ Banking, Financial Services, and Insurance (BFSI) business unit. He has extensive experience in advising senior executives across industries and geographies on transformation initiatives, business strategies, and IT solutions. Arora has an MBA degree from the Jamnalal Bajaj institute of Management Studies, Mumbai, India.