How to overcome GDPR implementation roadblocks with the help of automation

wipro

On 14 April 2016, the European Union (EU) approved the General Data Protection Regulation (GDPR), making it a law to replace the data protection directive 95/46/EC. The objective of developing a new privacy law was to harmonize data privacy laws across Europe, protect and empower all EU citizens of their data privacy and reshape the way organizations across the world approach privacy.

GDPR applies to all organizations involved in processing data of EU citizens anywhere in the world. Non- compliance with the regulation may result in fines up to €20 million, or 4 percent of overall global revenue of organizations processing personal data of EU citizens.

The GDPR, which came into force on 28 May 2018, is seen by many businesses as an obstacle to their smooth functioning. With organizational data having multiple entry points, data flowing from one process to another, data processing through various applications, and data stored across various databases, important question organizations face is a means to ascertain where personal data resides within their system.

GDPR: Implementation roadblocks

According to a survey conducted by crowd research partners in April 2018, it was projected that almost 60% organizations were at risk of missing the deadline for GDPR implementation. As part of the survey, organizations highlighted the following as the primary challenges for complying with the regulations:

• Lack of expert staff (43%)

• Lack of budget (40%)

• Limited understanding of GDPR regulations (31%)

The survey also highlighted that almost 56% of respondents expected their organization's data governance budget to increase in order to deal with the GDPR challenges.

GDPR has forced data privacy officers/ information security officers and boards of various organizations to redefine their data privacy strategy and to comply with the requirements of the regulation. Its adoption has become the biggest challenge for a majority of organizations, with effective implementation of controls and adherence being the major roadblocks. Organizations need to understand and track how personal data is being collected, processed, and stored.

GDPR has introduced certain key aspects, which organizations will have to consider while defining their implementation strategy. In most cases, organizations will have to perform the entire process of reaching out to respective business processes manually, and understand from them the various sources from where personal data gets collected. The process of gathering this information will be repetitive and will involve additional work-force and time to perform.

Automation to the rescue

How is it then that organizations can overcome this manual activity and in turn save time and workforce involvement? The solution to this seemingly daunting task lies in automating the manual processes that integrate with organization business processes, systems, and provides a deep dive view of all data and storage points.

Wipro has been successfully developing models and strategies for clients to reduce their operational cost and workforce, with its Enterprise Operations Transformation framework. Robotic Process Automation (RPA) is a major lever of the EOT framework and is capable of handling high-volume, repeatable tasks. RPA can assist clients to automate their GDPR journey by managing several critical aspects to comply with GDPR requirements such as:

1. Personal Information Management

• **Identify-** Mapping of existing data and new data across various business processes

• **Classify-** Assist in classifying personal information across the organization based on its sensitivity

• **Erasure-** Upon request from data subject for deletion of personal information across organiza-tional systems, the system may effectively track where the personal information resides and can be automatically be deleted

• **Anonymous-** Use a pseudonym or tokenize personal information wherever required

2. Consent

A third-party application can be integrated with RPA solution for customer correspondence and consent management.

3. Breach notification

Notify data subject of data breach within 72 hours in case any breach has been noted.

GDPR compliance through SAIX

At Wipro, we understand the challenges that organizations face while adhering to GDPR and are committed to transforming our clients' GDPR compliance journey by automating the most complex tasks of data inventory management, consent management, data portability request, and data breach monitoring through our framework.

As part of our transformation offering, we rely on "SAIX" model for defining solutions for our clients. "SAIX" stands for:

- **Simplify-** Standardize, Digitize, and Streamline processes
- **Automate-** Reduce the number of manual, rule intensive, high transaction based tasks and processes
- **Intelligence-** Incorporate actionable insights into organization business processes DNA with predictive and prescriptive analytics
- **Experience-** Reimagine the experience based on customers and internal stakeholders

Here is how the SAIX model aligns with the GDPR compliance automation (Figure1).

Wipro's 4 phase approach

Wipro can help its customers automate their GDPR compliance journey in four phases:

Gather

- Understand the type of personal data being processed
- How users are granted access to data and application
- Understand how data inventory is managed

Pre-assessment

- Wipro will assess the current state of the organization, based on the GDPR requirements and will accordingly suggest areas of improvement

Design

- Develop an implementation roadmap
- Define security requirements to be embedded
- Define rules based on data sensitivity and holding period
- Define customer portal view based on region and type of information collected, process, and stored data

Post-assessment

- Post implementation of GDPR automation solution, Wipro can help clients either perform a one-time assessment based on GDPR requirements under the compliance-as-a-service framework, or can perform a periodic review on the current state of organization controls based on GDPR requirements, and suggest recommendations if any.
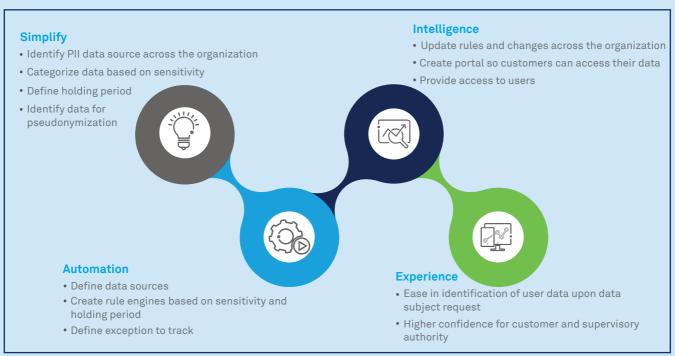

Simplify
- Identify PII data source across the organization
- Categorize data based on sensitivity
- Define holding period
- Identify data for pseudonymization

Intelligence
- Update rules and changes across the organization
- Create portal so customers can access their data
- Provide access to users

Automation
- Define data sources
- Create rule engines based on sensitivity and holding period
- Define exception to track

Experience
- Ease in identification of user data upon data subject request
- Higher confidence for customer and supervisory authority

Figure1: SAIX model alignment with the GDPR

GDPR's impact across industries

01 Finance

Customer Data
- Various applications
- Multiple touchpoints

Activities/process
- Customer onboarding process
- Relationship management
- Trade booking
- Accounting

Impact areas
- Client consent
- Right to data erasure
- Pseudonymisation
- Consequences of breach

02 Healtcare

Customer Data
- Various applications
- Multiple touchpoints
- Computer IP addresses

Impact areas
- Personal data flows
- Cross- border data transfer
- Privacy and security monitoring
- Consent management
- Right to erasure of data

03 Telecom

Customer Data
- Various applications
- Multiple touchpoints

Activities/process
- Data warehousing
- Reporting
- Marketing
- Inventory of data set

Impact areas
- Client consent
- Right to data erasure
- Anonymisation
- Data portability

04 Travel

Customer Data
- Various applications
- Multiple touchpoints
- Travel across different continents

Impact areas
- Consent management
- Personal data flows
- Cross-border data transfer
- Right to erasure of data
- Data breach notification

Conclusion

Automation for GDPR compliance will help organizations:

- Seek explicit consent on the data set identified for collection, processing, and storage
- Adequate data management through logs
- Maintaining adequate data inventory providing details of applications and databases where personal data is stored
- Pseudonymisation/ tokenization of personal data
- Face any regulatory audit effectively

About the author

Vinit Sinha
Associate Vice President – Compliance-as-a -Service, Wipro Limited

Vinit is an information security, data privacy and cybersecurity professional with over 12 years' experience into operations, consulting and auditing information security/ cybersecurity standard and framework. Vinit drives Wipro's endeavor of enabling organizations to strengthen their control environment to prevent data breaches and cyber-attacks. Vinit has deep domain understanding from varied experience serving across IT/ITES, business process management, telecom and others on developing effective risk management strategies.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**