Data Privacy Four Steps to Quickly Achieve GDPR Readiness

Abstract

As the European Union's General Data Protection Regulation (GDPR) takes effect on May 25, companies that collect data on citizens in these countries will need to comply with strict new rules around protecting customer data. With more than 99 articles, the GDPR will impose strict standards on enterprises and organizations to protect the personal data of EU residents.

To achieve GDPR readiness quickly, companies have a two-fold responsibility—they must take appropriate technological and business measures to set their house in order and identify the privacy and security risk areas within the work processes, and then proceed with addressing specific GDPR articles. Thus, companies should, first, initiate an organization-wide risk assessment of data privacy to identify those applications and processes that handle the maximum personally identifiable information (PII) of individuals. The next step should be to select the key contributors to privacy non-compliance, such as, the absence or lack of data security, and privacy-by-design measures, and address them through a four-step approach that we recommend based on TCS' experience in this domain.

Data Protection Laws Get Stricter

The General Data Protection Regulation (GDPR) marks the biggest overhaul of data privacy laws in the European Union (EU) in over two decades. Harmonizing 28 national legislations into a single directive, the GDPR is expected to set a new standard for consumer rights regarding personal data. Failure to adhere to these standards could see businesses being subjected to harsh penalties, ranging up to 4 percent of their global annual turnover.

Addressing GDPR is a top priority among affected companies, yet Gartner predicts that even by the end of 2018, more than 50 percent of them are unlikely to be in full compliance with its requirements[1]. As controllers or joint controllers of data, organizations must address privacy and security concerns while processing in-house the personally identifiable information (PII) of data subjects or customers, employees, and vendors. Their contractors and sub-contractors, who work as data processors, are equally responsible for compliance and must follow the same practice. At no point should the information identifying an individual be accessed, profiled, or shared without a clear and stated purpose, the consent of the data subject, and efficient security controls. Indeed, companies that service customers in the EU or employ workers from the region must leverage the golden opportunity of GDPR compliance to set their own house in order and swiftly streamline their systems and processes.

Cohesive Approach for Rapid Action

ITo ensure compliance with the GDPR as well as local data privacy laws, companies must first comprehensively re-examine their business processes, as well as data management practices when dealing with PII. In this regard, a judicious approach would be to select the most important of all the compliance regulations, and quickly achieve them to show maximum compliance in the least possible time.

To begin with, companies should initiate an organization-wide risk assessment of data privacy to identify those applications and processes that handle the maximum PII of individuals. The next step would be to focus on the major factors contributing to privacy non-compliance. Figure 1 depicts the outcome of GDPR privacy assessments conducted by TCS for more than 1000 applications that process large volumes of PII data across four major industries. It is clear from the data that the top two contributors to GDPR non-compliance are: the absence or lack of data security, and privacy-by-design measures. These two factors can form the takeoff point for the remediation journey for enterprises targeting quick regulatory compliance.

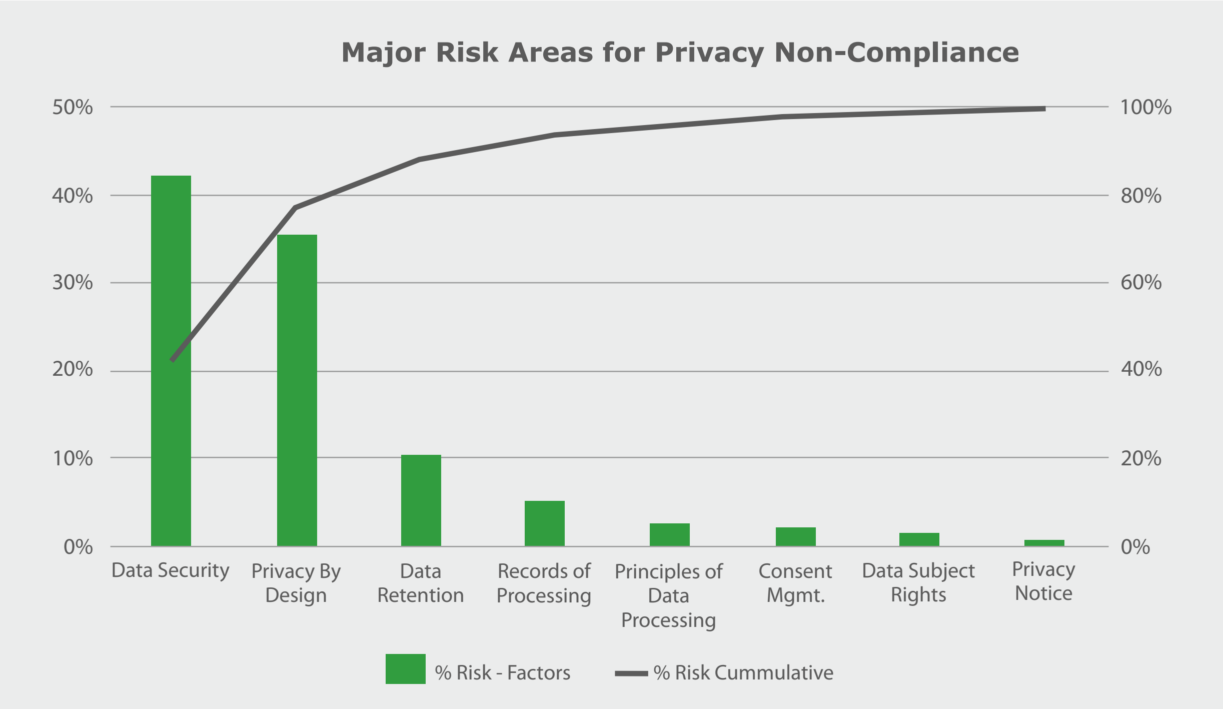

Figure 1: The risk areas for privacy

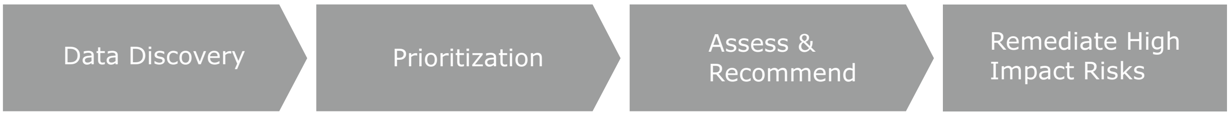

Figure 2. The four-step approach to compliance

Four Steps to GDPR Compliance

To meet these two goals as swiftly as possible, organizations need to follow a phased and time-bound strategy. Based on TCS' experience of successful data privacy and security engagements with clients, we offer a four-step approach that will enable organizations to quickly achieve GDPR readiness (Figure 2).

- **Discover PII attributes and purpose of processing:** Identify the individual personal attributes or user data that are collected, stored, or processed every day by the organization, in a structured or unstructured format.
- **Prioritize business processes/applications that handle PII:** Select business processes and/or applications using huge volumes of personal data and prioritize them for GDPR readiness evaluation.

- **Conduct privacy impact assessments to identify privacy risks:** Assess privacy impact to understand the risks related to the privacy and security of the data handled by the prioritized business processes and applications.
- **Implement solutions to remedy risk:** Identify and implement technical or procedural solutions across the organization to remedy cases of widespread, high-impact risk.

Streamlining Organizational Privacy and Security

GDPR compliance must be achieved in its entirety. Organizations could establish core groups to work on streamlining their own data privacy and security processes within the organization. To minimize any adverse impact arising from noncompliance, companies must customize key areas through packaged data privacy and data security solutions. These include:

Privacy notices: This document should list all details about the collection, storage, processing, and deletion of PII, along with the contact information of support personnel such as a data protection officer.

Consent management and data subject rights[2]: Implement solutions, preferably by the data controller, to manage consent from data subjects and enable them to execute their rights toward their PII.

Test data management[3]: Implement privacy-by-design measures to ensure that access to PII is governed by role and purpose.

Data masking and data security: Identify and implement privacy and security measures in both applications and business processes.

Data protection officer: Appoint a data protection officer per the GDPR mandate for all organizations processing PII of EU residents.

Formalize data protection impact assessment (DPIA): Streamline DPIA for all applications processing large volumes of PII data.

Review policies, procedures, and vendor contracts: Update and refine organization-level policies and procedures on information privacy and security, including contracts highlighting approved processing of PII by vendors and data processors.

Conclusion

GDPR is set to trigger widespread changes in the way organizations and industries are working with the personal data of employees, vendors, and customers. Adopting these safeguards would also prepare them for the future, as the solutions implemented to meet privacy laws can be cross-leveraged to improve their own security maturity and posture. To be in step with the dynamic world of data privacy, organizations processing customer PII data would do well to strike alliances with leading IT organizations providing centralized services in the cyber security consulting and solution areas.

References

1] Gartner says organizations are unprepared for the 2018 European Data Protection Regulation, May 3, 2017, https://www.gartner.com/newsroom/id/3701117, Accessed May 7, 2018

2] TCS Crystal Ball application offers an easy-to-install addition to any legacy application that lacks essential privacy control and improves system security.

3] TCS MasterCraft DataPlus tool helps organizations create privacy safe test data in non-production environments and ensure privacy of data at the juncture of data exposure in production environments.

About The Authors

Geo John

Geo John is a Data Privacy Consultant with TCS' Cyber Security group. With over 14 years of experience in the IT sector, he leads several data privacy and security compliance engagements with TCS clients across industry segments.

Hussain Mirza

Hussain Mirza is a Data Privacy Consultant with TCS' Cyber Security group. With over 11 years of experience in various IT roles, he conducts data privacy and security risk assessments and audits across industries and recommends solutions.

Contact

Email: cyber.security@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

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^{TM}, 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

TCS Design Services I M I 05 I 18