TATA CONSULTANCY SERVICES

Building on belief

Protect personally identifiable information with data privacy measures

Abstract

Across the world, organizations are mandated by specific data protection regulations and business domain-specific regulations to safeguard the personally identifiable and other sensitive information that they collect from their customers. These regulations pose stringent expectations on the way customer data is collected, stored, processed, used, moved, or shared. With business operations increasingly going global, organizations must wade through a complex ecosystem of regulatory compliance. The COVID-19 pandemic has only made data privacy requirements even more challenging to adhere to.

This white paper puts the spotlight on some of the basic data privacy measures that organizations can contemplate, if not envisioned already, to design an integrated and scalable data privacy framework.

Introduction

The COVID-19 pandemic times will go down in the annals of history as the ones which saw organizations face significant disruption in the way they executed their frontend business and backend operations. The pandemic waves have made organizations do the unthinkable – allowing their workforce to either operate exclusively from their homes, or at a minimum, distribute their working hours between home and office. Thus, with individual homes turning into mini-offices and organizations' need to ensure privacy of data of their internal and external stakeholders, data privacy challenges have reached unprecedented levels. However, it is important to recognize that the requirement of implementing data privacy controls was prevalent even prior to the outbreak of the pandemic, and this requirement will persist in post-pandemic times as well. The pandemic has only given an additional thrust to the faster adoption of data privacy controls.

Contemporary factors influencing data privacy in organizations

Considering the growing expectations on global organizations to increase focus on data privacy, here are some present-day factors that impact the organizations:

- **Proliferation of data protection regulations:** The list of countries in the process of adopting data protection laws keeps growing. Even countries having such a law already in place, are also working toward upgrading the law, in response to the changing needs of citizen data privacy and technological advancements. Some nations (E.g. Australia, Canada, South Africa, Japan, South Korea, and China) have their respective national data protection laws, the European Union has adopted a common law applicable to all countries in the region, and in countries such as the

US, individual states may have their own regulations. Countries may also have business domain-specific (e.g., finance, healthcare) data protection requirements. Many organizations do their business globally, in terms of their customer base, subsidiaries, and partner entities. Furthermore, regulations require that organizations must take consent from their customers before their data gets used / processed in a certain way. All these aspects make the entire data protection regulatory ecosystem extremely convoluted.

- **Broader scope of information privacy:** Traditionally, data privacy has been looked from the standpoint of the customers of an organization. However, in addition to customers, an organization engages with several other business entities, and the privacy of data related to these additional entities must also be protected. Such entities may include vendors, suppliers, partners, subsidiaries, and the organization's own employees, among others. Therefore, organizations must broaden their focus to include data of all such entities in the ambit of their data privacy requirements.

- **Data quality for data privacy:** The best efforts for ensuring data privacy will prove futile if the said data itself is inaccurate, incomplete, or inconsistent because such data has no business value. Even worse, an organization would invest in ensuring the privacy of data, which is not even applicable to their customers. Aspects related to the 'quality' or 'integrity' of data figure in some globally recognized data privacy frameworks and regulations (E.g. **Data Privacy Principles from OECD, APEC Privacy Framework, GDPR**, etc.). Organizations need to ensure that quality of their data is at the desired level and fits for the purpose as a part of their data privacy compliance initiatives.

- **Cloud adoption:** As a digital-driver, cloud is witnessing an accelerated adoption, owing to the changes in the way organizations are now running their business. While applications and data are getting moved to cloud increasingly, this transition is in a state of flux. Applications and data may be spread across cloud and on-premises. This necessitates implementing data privacy consistently across cloud and on-premises application data stores.

- **Data privacy supplementing data security:** Data security measures are typically directed towards a malicious agent that operates outside the organization's ecosystem while data privacy measures are targeted towards a malicious agent that could operate from within the organization's digital boundaries. Thus, organizations need to adopt the 'data-security-and-privacy' mindset rather than choosing between the two for the holistic protection of data.

- **Data privacy assurance:** Data governance requirement entails that data privacy measures should be measurable for their effectiveness. Organizations must be able to measure, track, and alert about key data privacy operational parameters, e.g. the level of coverage of data anonymization across different lines of business, data anonymization scores, risk of reidentification, information retention periods, citizen consents, and citizen age, among others.

Next-generation data privacy compliance framework

Organizations can consider implementing the following data privacy measures by not only looking at the current pandemic-originated needs but also for a long-term and strategic focus on data privacy. These measures are not to be considered as 'universally adequate'. Instead, these measures would be the bare minimum for organizations to enable data privacy:

- Organizations can look at data privacy compliance as an integrated objective to be achieved, as opposed to finding discrete solutions of compliance for each applicable country-level or domain-specific regulation. This could be a daunting task. However, upon closer inspection, it is evident that most data protection regulations echo the same basic sentiments as some commonly recognized and foundational data privacy principles. Finding piecemeal solutions is not a scalable approach, as more countries adopt data protection regulations, and many countries upgrade their existing laws. Instead, organizations can look at establishing an integrated data privacy framework, which factors into account the asks of all applicable regulations. This framework should help choose the most stringent requirement by default against a given dimension of data privacy (say, period of data retention), leaving open handles for customization, depending upon the nature of business and the particular law and geography in scope. A policy-driven approach can help ensure ownership, auditability, and governance.

- A formal consent management framework assures organizations that only the required data, and nothing more, is collected from customers with their explicit consent for the specified purpose of processing and the duration of usage.

- Organizations can transcend from an ad-hoc approach of data privacy to an institutionalized, governed, and organization-wide data privacy program headed by a role akin to Chief Privacy Officer, with direct reporting to the CIO (at least) or CEO (preferably). Organizations can form a 'core data privacy committee', with representatives from all key organization functions, such as sales, marketing, branding, HR, administration, legal, internal IT, governance, risk and compliance, operations and product/service delivery, for a more cohesive outlook toward information privacy.

- Organizations can demonstrate adherence to some internationally recognized standards such as the **ISO 27000, ISO 27001, ISO 27002, ISO 27018, ISO 29100,** and/or recognized data privacy seals. Attestation from independent agencies, validates an organization's commitment toward data protection and instills trust with internal and external stakeholders.

- Organizations can try to implement the principles of data privacy by design and by default. Data privacy can neither be an afterthought nor some obligatory actions executed merely to avoid being deemed as 'non-compliant' by the regulatory bodies. Rather, the elements of data privacy can be at the very heart of design and architecture of products, solutions, platforms, applications, and systems.

- Organizations can favor a software-driven approach to data privacy throughout the data's lifecycle and eschew any shortsighted approaches that involve either manual operations or highly tailormade, script-driven solutions that have a small chance of horizontal and vertical scalability. The software itself should be usable in a self-service mode with its operations automated through ML and AI. Technologically, the software should be capable of supporting structured, semi-structured and unstructured data sources that could reside on-premises or on cloud. To answer the expectations of data privacy assurance, the software must define, measure, and monitor key operational metrics and support the necessary reporting/dashboarding either natively or by integrating with other software.

- For organizations to implement reasonable data privacy controls, they can first answer the question: What data in data repositories can be treated as personally identifiable or sensitive, and where is such data located? This calls for an automated approach of discovering direct and indirect sensitive business data elements, from both structured and unstructured data formats, within the organization's data repository. Once discovered, methods such as setting up of data dictionary, data classification, and data lineage can be employed to gain a deeper understanding of data categorization, inter-relationships, and its movement. This is critical, especially, considering the data residency and movement restrictions imposed by data protection regulations. Importantly, the scope of this exercise is not just sensitive customer data, but also includes sensitive data of other entities that the organization engages with for business purpose.

- Once the organization has gained insights into the nature of sensitive business data elements that it acquires, generates, stores, processes, and shares, it can implement a combination of one or more privacy enhancing technologies such as static data masking, dynamic data masking, data pseudonymization, and even modern approaches such as differential privacy. By combining the powers of such traditional and modern technologies, organizations can meet their requirement of privacy-safe data provisioning, usage, and access, for traditional and modern usage scenarios alike. Again, the appropriate use of such technologies applies to sensitive customer data and sensitive data of other entities that the organization engages with for business purposes.

- Organizations can explore setting up a role-driven approach of accessing information, using the dynamic data masking technology for a stronger inward-facing data privacy. This ensures that the information is accessed on a 'need-to-know' basis, even by the internal stakeholders, thereby reducing the risk of malicious use of data.

- It will help organizations if data privacy and data quality needs are handled in a consolidated manner through both types of software working in an integrated fashion. Integrated approach of data privacy and data quality measures will allow organizations to get a 'bigger picture' of the state of compliance of their data.

- In addition to working closely with data security and data quality management software, a data privacy software must be amenable to interaction with neighboring software/applications in the enterprise's IT ecosystem. This could include DevOps, agile, identity and user entitlements management, data management, data governance, data analytics, risk and compliance and such software or applications. This is required as the aspects of data privacy span a whole gamut of data processing activities and various touchpoints where users interact with data.

- Organizations can watch out for evolving trends in the data privacy domain. Data protection regulations now espouse requirements such as data portability and the right to the erasure of information which reflect modern sensibilities of data privacy.

Conclusion

The very term 'data privacy' seems to have an almost oxymoronic tint to it. How could an entity, whose very purpose is to generate business value, through its collection, processing, transformation, and sharing, be kept 'private'? Organizations will continue to bank on data to further their business. Also, with citizens becoming increasingly concerned about safeguarding the privacy of their data, organizations need to bolster their data privacy measures. Data privacy is more about organizations collecting only the strictly essential data of citizens and using it in a legally compliant, fair, secure, consent-driven, purpose-limited and time-limited manner. It is no longer a choice but an imperative for the sustenance of an organization's business and gaining customer trust.

About the authors

Ashim Roy

Ashim Roy is the Global Product Head of TCS MasterCraft™ DataPlus, which is an integrated data management software from TCS. Ashim carries more than 26 years of industry experience in business verticals such as Manufacturing, Investment Banking and IT industry. Ashim pursues his interest in enterprise product development, particularly, in the area of Data Privacy and Data Quality and has 10+ patents under his name. Ashim holds a master's degree in Robotics from IIT, Kanpur.

Sumeet Bhide

Sumeet Bhide handles Market Research, Marketing, Learning and Development aspects of TCS MasterCraft™ DataPlus product. He has around 20 years of experience in TCS. He has successfully delivered some key IT projects in the areas of reengineering and migration. His areas of interest include Data Management, Test Data Management and Data Privacy. He holds a Bachelor of Engineering degree in Electronics and Communication Systems Engineering, from Gujarat University, India.

TATA CONSULTANCY SERVICES

Awards and accolades

TOP 3
IT SERVICES
BRAND

FASTEST GROWING
IT SERVICES BRAND
FOR THE DECADE
2010 - 2020

Contact

Visit the TCS MasterCraft™ page on https://mastercraft.tcsapps.com/dataplus

Email: mastercraft.sales@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS**.

Corporate Marketing | Design Services | M | 02 | 22