Data privacy – are you ready?

Data governance knowledge series – Topic 4

December 2019

pwc

Need for data privacy

As data becomes crucial for enterprises and governments around the world, there has been a multifold increase in the volume of data being created, stored and processed, resulting in it becoming a critical commodity. India is gradually emerging as a data-driven economy. As per a report by the Telecom Regulatory Authority of India (TRAI),[1] as of June 2019, out of 665.31 million internet subscribers in India, 21.67 million were wired internet subscribers and 643.64 were wireless internet subscribers. These numbers indicate that personal data is becoming available in the public domain due to high mobile internet usage. Statistics show that 30.5% of Indians are below the age of 25[2] and extensively use mobile apps to access social media. Therefore, it becomes imperative for the government to protect personal data of its citizens.

Different countries have enacted data protection laws and regulations, such as the General Data Protection Regulation (GDPR) for citizens of the European Union (EU) and the California Consumer Privacy Act (CCPA) for residents of California.

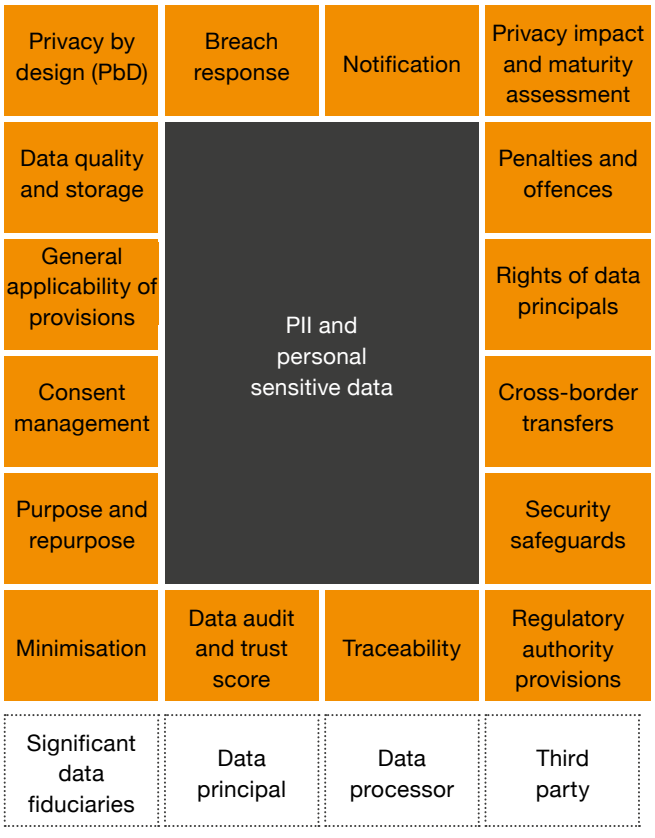
The Personal Data Protection (PDP) Bill, 2018,[3] is slated to become India's first proper Legislation on data protection. The draft of the bill is based on recommendations on data protection and privacy by a government-constituted panel.

In this article we will not be explaining the Indian data privacy law but identifying areas of the law, which data governance and technology can help to comply.

The PDP Bill touches upon various aspects of information lifecycle, as shown in Figure 1. The draft bill states that the government will have jurisdiction over the processing of personal data, if such data has been used, shared, disclosed, collected or processed in India. The government will also have jurisdiction over the personal data collected and processed by the companies incorporated under Indian law, irrespective of the place of origin of the data.

The five action areas defined in Figure 1, when implemented, would help an organisation be compliant with data privacy laws. In the subsequent sections, we will further explore these action areas.

Figure 1: Information lifecycle of data



Action Areas

Governance (policy and process)

Establish governance programme to manage, secure and control personal data related policies and processes.
Areas covered: PbD, purpose and repurpose, data audit and trust score, privacy impact and maturity assessment, security safeguards, regulatory authority provisions, penalties and offences

Consent architecture

Obtain express consent for collection, storage, processing, disclosure and movement of personal data.
Areas covered: Consent

Data lifecycle management

Implement secure data collection, processing, storage, sharing and archival/disposal controls.
Areas covered: General applicability provisions, data quality, data storage and traceability, minimisation, cross-border transfers, PbD, security and safeguard

Rights management

Fulfill data principal requests with regard to access, modification, destruction, data portability, rights to forget, etc.
Areas covered: Data principal rights, cross-border transfers

Notification and breach response

Notify breaches to the data principal and data privacy and protection authority
Areas covered: Breach, notification

1 https://main.trai.gov.in/sites/default/files/PIR_01102019.pdf
2 http://censusindia.gov.in/Census_And_You/age_structure_and_marital_status.aspx
3 https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

Role of data governance in data privacy

Data governance and data privacy go hand-in-hand. Although data governance doesn't solve all data privacy requirements, it helps cover a lot of ground for compliance with privacy regulations. A good governance operating model helps to ensure that compliance is put in place across the organisation suitably. Data governance office (DGO) is now a major requirement for various data privacy compliances such as GDPR in the EU and a similar office will also become a primary requirement for India's data privacy laws. A comprehensive data governance policy sets appropriate data monitoring processes and metrics in place to ensure smooth functioning of business, while meeting data compliance requirements.

Data privacy laws mandate that organisations know and record where their data resides, who uses the data, how the data is used and how the organisation's business process is related to the data. An effective way for organisations to ensure compliance with such regulations is to build a comprehensive data inventory and data map that identifies the necessary criteria of compliance. Data owners and data stewards can record such information as business and technical metadata, tagging and mapping it with business processes to facilitate transparent data lineage and data mapping.

Data classification is another method used for data governance and to protect data privacy and meet regulatory requirements. With the help of data classification, organisations can adopt proactive measures to ensure compliance with regulatory requirements. Data can be classified and categorised based on data access frequency, user activity, volumes, etc. This can enable risk-based prioritisation of any data privacy-related issues and identify gaps in the current data.

The data access component of data governance can help address data security risks. Drafting clear and definite access guidelines for both internal and external exchange of data can help control data flow and ensure that only authorised parties have access to the data. It is also necessary to evaluate and continuously monitor all the security risks to have a greater control on information. Data-to-process and data-to-role relationship matrices are some of the ways to manage data access.

Role of technology in data privacy implementation

Various technological solutions can be used to achieve the goal of data privacy and compliance in an organisation. These technologies cater to regulatory needs related to data privacy and protection and ease the functioning of organisations. Some of the scenarios where technological solutions can help the organisation comply with various regulatory requirements are discussed below.

Meeting compliance requirements such as consumer rights and consent management

With the help of available tools and technologies, organisations can identify sensitive data and classify it as personally identifiable information (PII) data, which in turn helps in authorising access requests by data subjects. Central data storage systems can be utilised for simpler, faster and more reliable data analysis and auditing of the data in real time, to ensure that consent is in order.

Personalised dashboard with compliance score

Business executives can get access to personalised dashboards to gain insights into business metrics that relate to database safety and get the compliance score for their organisational data to ensure that data collection, storage and usage are as per regulations.

Flexible data access governance

Data access governance tools can help in providing visibility into the type of sensitive data stored, its location, and who holds what type of rights and access over the data, thus allowing organisations to manage data access permissions to enforce least privilege.

Data lineage to track data processing activities

Data lineage helps in keeping a check on the data processing activities. With the help of various tools available today, data repositories and resources can be scanned, and sensitive data can be identified and classified by organisations so as to adhere to compliance regulations. Technology can help organisations to automate the decision-making about data deletion, archival, optimisation of data and data governance.

Enabling notification and breach response

A key requirement of data privacy laws is to ensure that data principals are aware of the purpose and nature of data usage, along with the details of personal data with an organisation. In case of a data breach, the relevant authorities must be informed and based on severity of the breach, data principals may also need to be informed.

It is becoming increasingly important for organisations to integrate communication channels such as email, SMS, call centres and webpages and centrally manage such channels so that data principals can be informed about breaches. Solutions, based on predefined rules, are also available for identification of data breaches. Leveraging such technologies can enable organisations to respond to incidents of data breaches quickly and efficiently.

Tools and technologies which can assist in ensuring data privacy and managing data efficiently in its lifecycle journey are:

- database management systems
- business intelligence tools
- application frameworks
- identity management technologies
- change control systems
- access and authentication systems
- workflow management solutions
- usage management solutions
- data discovery and cataloguing solutions
- security solutions
- data lineage tools.

Data privacy enablers

For organisations to wholly comply with data privacy laws, restructuring is often required. For example, systems and technological solutions in an organisation should be designed in such a way that they ensure: (i) data processing is limited to the purpose for which the data was collected; and, (ii) access to personal data is granted only to those who need it. Also, an automated consent management framework would help in easy and error-free management of requests related to PII data.

Data privacy by default or design

For organisations to comply with strict privacy standards and have greater control over data, there is a need to adopt the principle of PbD, along with privacy by default. Privacy by default is a product-related approach which requires controls to be put in place across all the data collection points. It implies that once a product or service has been released to the public, the most stringent privacy settings are applied by default, with no manual intervention from the end user. PbD requires the organisation to make robust privacy policies which reflect in both technical and business conduct. PbD can be achieved by:

- implementing a privacy impact assessment for each system across the organisation.
- having a standard risk assessment procedure in place to deal with breaches and issues.
- reviewing and updating data life cycle management techniques.

Consent management framework

An automated consent management framework is an enabler which addresses the challenge of customer trust with respect to their personal data and information and adds to customer delight. This framework is a customer touchpoint and is used to raise, validate and process requests raised by customers. Given that post-implementation of the data privacy law in India, an organisation would need to process multiple requests to update and delete PII data, an automated solution based on a well-defined framework would provide a quick, secure and accurate turnaround time for such requests.

Conclusion

In order to comply with data privacy laws, organisations would need to change their policies and practices on data management. A sound data governance framework and technological solutions are the two major drivers in an organisation's journey towards compliance. Organisations must have in place policies to ensure checks and balances for every data transition which takes place during the information journey. Organisations would also require solutions to identify PII data across application landscapes and execute appropriate action, based on client requests and principals of data privacy laws. Automated consent management to manage multiple PII data-related requests is the need of the hour. Technology solutions can also help organisations address concerns related to data security. A central communication channel, established with data principals, can certainly go a long way towards ensuring clients' trust and compliance with data privacy laws.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Acknowledgments

This knowledge series has been researched and authored by Abhishek Chaurasia, Aditi Tripathi and Samiksha Wahi.

Contact us

Mukesh Deshpande
Data Management Leader
Partner, Technology Consulting
mukesh.deshpande@pwc.com
+91 9845095391

Amit Lundia
Data Governance Leader
Director, Technology Consulting
amit.lundia@pwc.com
+91 9836922881

pwc.in

Data Classification: DC0

SG/December2019-M&C3708