IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

"Compliance Challenges before Indian Businesses under the Digital Personal Data Protection Act, 2023"

Adv. Yatin Pandit

Visiting faculty

TMC Law College, Thane

Abstract:

This paper is focused on introduction of Digital Personal Data Protection Act, 2023 ("DPDP Act") in India and the probable compliance challenges which may be faced by Indian Businesses while complying with provisions of the DPDP Act. Indian businesses will witness a shift in data governance and privacy regulations on the similar lines with General Data Protection Regulation ("GDPR") of European Union. With the advent of technology, Indian businesses have started collecting Digital personal data of individuals and storing such data for future references. Such storage and process of data without consent may create problems like data theft, misuse of data etc. So, the introduction of DPDP Act is a welcome step to safeguard digital personal data of individuals while promoting economic growth.

It is well settled principle of law that *"when there is right, there should be corresponding remedy"*. There are strict provisions under the DPDP Act for data handling and data processing which may pose compliance challenges for Indian Businesses such as data minimization, encryption, consent requirements, transfer of data to outside India etc. In case of non-compliances, Indian Businesses will be facing harsh penalties. To overcome all these challenges, Indian Businesses will have to build effective data protection mechanism within the organization which may definitely add cost in near future.

The DPDP Act has also mandated Consent requirements from Data Principals before collecting and processing their data. Few prescribed Business entities will have to appoint specialized Data Protection Officers (DPOs) within the organization to ensure due compliance of the DPDP Act provisions from time to time. One of the biggest challenges Indian Businesses may face with regards to skilled workforce to

understand and educate internal stakeholders about the DPDP Act compliances. There is no doubt this may become an additional burden especially on Micro, Small and Medium-sized enterprises (MSMEs).

Though DPDP Act may become challenge for Indian Businesses but it will bring reforms in data governance in todays digital era. Indian Businesses will have to understand compliance requirements of the DPDP Act to mitigate the risk. This will definitely build competitive advantage for Indian Businesses worldwide.

Keywords:

Compliance challenges, Indian Businesses, Digital Personal Data Protection Act, 2023 ("DPDP Act"), GDPR, Data protection.

❖ Objectives

- Historical Background of Data Protection laws in India
- Introduction of the Digital Personal Data Protection Act, 2023 ("DPDP Act")
- Key Provisions of the DPDP Act
- Probable Compliance Challenges for Indian Businesses
- Case Studies on non-compliance of Data protection laws
- Strategies for Overcoming Compliance Challenges

❖ Research Methodology

The research paper is an exploratory research, based on the secondary data sourced from website, statues, journals, magazines and articles. Looking into requirements of the objectives of the study the research design employed for the study is of descriptive type. Available secondary data was extensively used for the study.

❖ Historical Background of Data Protection laws in India

The roots of Data Protection law can be found in the Information Technology Act, 2000 ("IT Act") which was the first law enacted in India to recognise provisions on confidentiality, privacy and security for information stored in a computer. The Department of Information Technology under the Ministry of Communication and Information Technology ("Meity") notified the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") on 11th April, 2011, which were issued under the IT Act to protect Sensitive Personal Data or Information collected from Natural persons by Body corporate. The Data Protection Rules was the starting point to protect Sensitive Personal Data or Information in India.

Time and again the question was raised before the Supreme Court whether "Right to Privacy" is the Fundamental Right enshrined under the Indian Constitution ("Constitution"). In the Landmark judgment delivered by the Hon'ble Supreme Court on 24th August, 2017 in *"Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors"* Writ Petition (Civil) No 494 Of 2012 ("Puttaswamy Case") recognized the

existence of "Right to Privacy" as an intrinsic part of the right to life and personal liberty mentioned under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. It means though it was not expressly worded in the Constitution, by overruling earlier judgments, Hon'ble Supreme finally acknowledged the importance of Right to Privacy. So, like any other Fundamental Rights enshrined under Part III of the Constitution, Right to Privacy can be enforced against the State in case of its infringement. The Hon'ble Apex Court also opined that a data protection law to be framed by the State to protect individual's rights against private or non-state parties. Further, Supreme Court suggested that principles set out in this judgment should be taken into consideration while drafting the new data protection law in India.

❖ Introduction of the Digital Personal Data Protection Act, 2023 ("DPDP Act")

Post landmark judgment passed by Hon'ble Supreme Court in Puttaswamy case, Committee of Experts under the Chairmanship of **Justice B. N. Srikrishna** ("Justice Srikrishna Committee") was constituted in August, 2017 to identify key issues involved and further challenges around Data protection to propose suitable regulatory framework for Data protection in India. The Justice Srikrishna committee submitted its report named *"A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians"* to Meity on 17th July, 2018[1].

The introduction of the DPDP Act is more or less based on international practices of data protection. The General Data Protection Regulation ("GDPR") introduced by European Union was implemented in 2018. The GDPR set a benchmark worldwide for data protection and ultimately GDPR influenced many countries worldwide to introduce Data protection legislation in their jurisdiction.

The GDPR contains strict provisions for data processing, prior consent, rights of Data subjects, duties of Data Controller etc. The DPDP Act contains similar provisions with different nomenclature to protect digital personal data of individuals. At the same time, the DPDP Act has tried to maintain the balance by exempting certain provisions for national interests. The DPDP Act will definitely give boost to overall economic growth and technological development in India. The time has come when Indian businesses have to think to adopt strict provisions and prepare policies to comply with DPDP Act.

❖ Key Provisions of the DPDP Act

1. Consent Manager requirement

The DPDP Act requires express consent from Data Principal for processing their data. The DPDP Act also confers right on Individuals to withdraw consent at any time. Such withdrawal may disrupt ongoing data processing activities.

[1] Srikrishna, B. N. (n.d.). *A free and fair digital economy: protecting privacy, empowering Indians*. Committee of Experts. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

2. Data Fiduciary Obligations

Data Fiduciaries will have to ensure that digital personal data is collected only for specific lawful purpose and not otherwise. So, the Data Fiduciaries will be required to adopt adequate security measures to protect digital personal data of Data Principles.

3. Data Principal's Rights

Once Digital Personal Data is shared with Data Fiduciaries, Data Principal has right to correct the same. Additional protection is also provided to Data Principals if request is made to Data Fiduciaries for deletion of such Data.

4. Data Transfers outside territory of India

The DPDP Act imposes restrictions on the transfer of Digital Personal Data of Data Principals outside the territory of India, if such processing is related to offering of goods or services to Data Principals within the territory of India.

5. Data Protection Officer (DPO)

The DPDP Act mandates Significant Data Fiduciary to appoint DPO. The contact details of such DPO are required to be provided to Data Principles in order to access data or to respond to any communication from the Data Principal for the purpose of exercise rights.

6. Data Protection Board of India ("Board")

Under DPDP Act, the Central Government is empowered to establish Board which will act as a Regulator to safeguard the rights of Data Principals. The Board may also conduct inquiry by following the principles of natural justice. Further, the Board is empowered to impose monetary penalty as specified in the Schedule of DPDP Act in case post inquiry, Board determines breach of provisions of DPDP Act.

7. Penalties

The Schedule mentioned under DPDP Act provides list of stringent penalties ranging from minimum Rs. 10 thousand to Rs. 250 crores for breach of provisions of DPDP Act.

❖ Probable Compliance Challenges for Indian Businesses

Post implementation of GDPR, various Multi National Organizations had to comply with its provisions. But the DPDP Act will definitely bring compliance challenges for Indian Businesses which had not yet thought to build such infrastructure so far. There may be multiple challenges faced by Indian Businesses with respect to Technology, Financial, Organizational, Legal & Regulatory etc. We will try to understand these various compliances challenges in detail.

1. Technological Challenges

The DPDP Act may pose various Technological challenges for Indian Businesses with respect to Data Localization, Data Security etc. With the growth in technology, the barriers have been removed when it comes to storage of Data. Many Indian Businesses have already relied upon the international data centres for storage and its processing. One of the biggest challenges for Indian Businesses will be to store and process data within Indian territory. This Data localization requirements will not only create hurdles for Indian Businesses but also increase the cost in near future. The Indian Businesses may have to identify and invest into new local data infrastructure. This may potentially disrupt their existing partnerships with international data centres.

The DPDP Act mandates data security measures to protect digital personal data of Data Principals for ensuring compliance. This may be challenging for Indian Businesses which lack expertise or resources to implement advanced security measures. Such Indian Business will have revisit the budget to invest in new technology and training their workforce to comply with these requirements.

2. Organizational Challenges

The existing policies will required to be relooked by Indian Businesses to bring awareness about compliance requirements about DPDP Act.

The DPDP Act mainly focuses on data governance and accountability for data processing. Indian Businesses should plan out to establish clear policies and procedures for data processing. They should also ensure that not only employees but all representatives have understood the compliance requirements of DPDP Act. Considering the stringent penalties which may be levied for non-compliance, Indian Businesses may have to incur additional cost to create new roles within the organization.

The breach of provisions of DPDP Act by entry level employee may also affect the entire organization and so Indian Businesses will have to conduct regular trainings to ensure that compliance requirements of DPDP Act are well understood at all levels.

3. Financial Challenges

The Indian Businesses may witness significant financial investment once DPDP Act will be fully implemented. The Financial investment in the areas of data localization, software related to consent management, conducting training for awareness will have to be planned. In India, Micro, Small and Medium Enterprises (“MSMEs) have contributed immensely for economic growth of nation. But this additional compliance cost of DPDP Act will definitely affect the survival of MSMEs. Additionally, many technology Start ups are being set up by young entrepreneurs which are majorly working in sectors like Application development, E-commerce, cloud computing etc. To run such businesses, these Start ups are collecting and processing digital personal data of individuals on regular intervals. Such Starts ups which are always in need of funding will have to convince their Investors about compliance set up for DPDP Act.

4. Legal and Regulatory Challenges

The new Company law which was introduced in 2013 has already undergone many changes so far. Similarly, the DPDP Act may take some time to settle down as rules have not yet been notified. Indian Businesses may face various legal and regulatory compliances challenges with the DPDP Act. There may be lack of clarity in the initial phase of implementation of DPDP Act which may lead to unnecessary disputes and interpretation issues. The Indian Businesses may be required to invest time and resources for getting proper legal advice. Indian Businesses which are operating internationally and already complying with GDPR will have to additionally comply with DPDP Act. The Indian Businesses may have to redraft contractual clauses post implementation of DPDP Act.

5. Data breach notifications

Under DPDP Act, it will be responsibility of the Data Fiduciary to intimate personal data breach to the Board post its occurrence. Data Fiduciary is required to build mechanism for detecting, mitigating such data breaches. At the same time, timely intimation should be given to the Board. Indian Businesses dealing with large volume of digital personal data may find it difficult to assess the breaches and its further notification to the Board from time to time.

❖ Case Studies on non-compliance of Data protection laws

As mentioned earlier, DPDP Act has specified stringent penalties for non-compliance of its provisions on similar lines with GDPR. Let us try to understand what may happen in case of breach of personal data with the help of case studies.

1. Google's Data breach case in France:[2]

CNIL (Commission Nationale de l'Informatique et des Libertés) imposed a financial penalty on tech giant Google LLC for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization in accordance with GDPR provisions. There were two complaints received to CNIL alleging Google for not having a valid legal basis to process the personal data of the users of its services, particularly for ads personalization purposes. In order to deal with the complaints received, the CNIL carried out online inspections in September 2018. The aim was to verify the compliance of the processing operations implemented by Google with the French Data Protection Act and the GDPR. After investigation, CNIL's restricted committee responsible for examining breaches of the Data Protection Act observed two types of breaches of the GDPR viz. *1) A violation of the obligations of transparency and information and 2) A violation of the obligation to have a legal basis for ads personalization processing.*

[2] *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | European Data Protection Board*. (n.d.). https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

CNIL identified that Google failed to provide Data subjects with adequate information about data processing activities and did not obtain valid consent for said personalized ads. The Google data breach case is an eye opener for Indian Businesses as it shows importance to comply with data protections regulations while data collection and consent management.

2. British Airways Data Breach:[3]

This data breach incidence happened during 22nd June, 2018 to 5th September, 2018. In this data breach, almost 4,00,000 customers of British Airways were affected. Attackers gained access to an internal British Airways application and subsequently personal & financial data, including names, addresses, and credit card details were stolen by the Attackers. As soon as British Airways came to know of this data breach incident, it approached UK Information Commissioner's Office (ICO) on 6th September, 2018. The ICO considered that British Airways has cooperated fully with her investigation and has taken that into account. However, ICO found that *"British Airways failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and by Article 32 GDPR."* After taking into consideration range of mitigation factors applied by British Airways and due to the impact of Covid-19, the amount of the penalty that the ICO decided to impose was £20 million.

❖ Strategies for overcoming compliance challenges

After understanding above mentioned compliance challenges for Indian Businesses, effective strategies should be framed to overcome these compliance challenges. Indian Businesses may adopt following strategies and best practices.

a) Formulate data protection framework: Indian Businesses processing personal data may formulate comprehensive data protection framework which may include policy, guidelines for processing personal data to comply with DPDP Act. This comprehensive framework may include all necessary compliances such as consent management, privacy notice, Data Principal rights, Data Fiduciary obligations, roles and responsibility of DPO etc. Just formulating framework may not be enough and so Indian Businesses will have to review and update the same from time to time as and when there are new regulatory changes under DPDP Act.

b) Adopt transparent data practices: The DPDP Act mandates that Data Fiduciary to provide Data Principals with clear and concise information as to how personal data will be collected, processed and stored. So, Data Fiduciary may include all possible information in the privacy notices in simple English language or other language permissible under the DPDP Act. Effective communication to Data Principals on timely manner will definitely bring transparency required under DPDP Act.

[3] ICO. (2020). *PENALTY NOTICE*. https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf

c) Implementation of Privacy features in system: At the time of development or implantation of new technology or system, Indian Businesses may embed certain privacy features to automate the process. Compliances such as data minimization, specified purpose and security measures may be embedded in the system. Also, Indian business should avoid collecting personal data which is not required for specified purpose.

d) Implementation of security measures: Indian Businesses may adopt best and proven security measures to comply with DPDP Act. Many MNCs in India are already complying with GDPR and so similar best practices to implement security measures may be identified and adopted by other Indian Businesses. These security measures will help to protect personal data of Data Principal from unauthorized access, modification, disclosure or destruction.

e) Data Protection Impact Assessments (DPIAs) and periodic audit: The DPDP Act mandates only Significant Data Fiduciary to conduct DPIA and periodic audit. But Indian Businesses from the beginning may think to conduct DPIA and period audit internally though its not mandatory compliance for them. These activities will be helpful to mitigate the risk involved in data processing. DPIA should comprise description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals.

f) Appoint legal experts: Indian Businesses may think to appoint legal experts who are already having hands on experience in GDPR compliances. Such experts will be instrumental in drafting Data Processing agreement and can advise Indian Businesses on day to day compliance requirements under DPDP Act. These experts can act like Cost controller for Indian Businesses by saving huge penalties prescribed under DPDP Act.

g) Participate in Forums or Conferences: Indian Businesses may participate in various forums or conferences to understand emerging trends in the field of data protection. They may also come across best practices followed by MNCs for GDPR compliances. Deliberations with experts in such conferences will definitely help Indian Businesses to mitigate risk.

h) Conducting internal Trainings: Indian Businesses may think to conduct regular training programs to bring awareness about the data protection within the organization. Post conducting such training programs, reference material comprising compliance required under DPDP Act may be shared with employees. Additionally, employees may be compulsorily asked to appear for internal test for DPDP Act compliances.

❖ Conclusion

The DPDP Act comes up with challenges and opportunities for Indian businesses. With compliance of DPDP Act, we may see good data governance which may in turn enhance trust amongst customers. Indian Businesses will have to adopt best practices by keeping long term perspective.