Digital Personal Data Protection Bill, 2023

Divya Jain

October 2023

What is the need of Digital Personal Data Protection Act?

Facebook-Cambridge Analytica Scandal

In 2018, it was revealed that the personal data of millions of Facebook users had been harvested without their consent by Cambridge Analytica, a political consulting firm. This incident not only highlighted the potential misuse of personal data but also exposed the loopholes in data protection practices. It resulted in a public outcry and significant legal repercussions for both Facebook and Cambridge Analytica

Google's €50 Million Fine

In January 2019, Google received a hefty fine of €50 million by the French data protection authority, CNIL (Commission Nationale de l'Informatique et des Libertés). The fine was imposed for violating GDPR principles, specifically related to the transparency and lawfulness of processing personal data. CNIL found that Google failed to provide users with adequate information about data processing activities and did not obtain valid consent for personalized ads

Impact: 4.5 million Air India customers

In February 2021, hackers broke into Air India's database to steal the personal information of **4.5 million** Air India customers. The data compromise happened on the heels of another data breach at Akasa Air. After the incident, Air India sent emails to the affected passengers that the security of their data had been compromised and personal information such as user ID and password had been stolen. The hackers obtained sensitive information to access passengers' GST invoices and reveal it in the public domain. However, credit card information like CVC and CVV numbers were not stolen as claimed by Air India in response to allegations.

Air India Data Breach

Feb, 2021

Apr 2021

Upstock Data Breach

Impact: 25 lakh users

The security systems of Upstox, India's second-biggest stock broking firm with regard to the number of clients, were breached in April 2021 by hackers who obtained KYC and other information of **25 lakh** customers. According to a Times of India report, the data theft was traced to a third-party warehouse, and the documents were uploaded on the dark web.

The hackers responsible for the contravention allegedly belonged to a group called 'Shiny Hunters'. Investigators discovered that the hackers had obtained the Amazon Web Service Key to unearth account information.

Impact: 66.9 Crore

The confidential data of over 50,000 individuals who attended the police recruitment exam in December 2019 was violated by hackers. The information of participants like birth dates, cell phone numbers, candidate names, email IDs, FIR history, and criminal records, among others, was put up for sale by hackers. The information leak was discovered by CloudSEK when the hacker shared a sample of the stolen data with them. However, the 2019 data spill pales in comparison to the data theft of **66.9 crore people** in 2023. The incident came to light when Cyberabad police sent notices to 11 entities including three banks, an IT services company, and a social media behemoth, asking the company representatives to present themselves before them in pertinence to the massive data leak. The Cyberabad police reportedly arrested one Vinay Bharadwaj for thieving, storing, and selling the personal information of 66.9 crore people and companies across India.

Police exam data spill (2019) and Cyberabad data theft (2023)

2019 and 2023

Apr,2021

Domino's India Data Theft

Impact: 18 million orders

The Indian arm of Domino's Pizza revealed in April 2021 that a threat actor had hacked their database and sold the compromised data on a hacking forum. The actor claimed to have laid their hands on **13 TB** of information comprising data of 18 million orders reflecting customer names, addresses, delivery locations, and phone numbers, along with the credit card information of 1 million individuals from the database of Domino's India. However, the pizza chain claimed that customer credit card data wasn't compromised as they don't maintain the financial records of their clients.

Impact: 80,000 users

Through a string of cyber-attacks on government websites in 2021, hackers managed to lay their hands on a database that comprised the personal data of approximately 1500 Indian citizens. The hackers rendered the data public through PDF files that were available for download. It was further discovered that the agencies responsible for the onslaught were based in New Delhi. Likewise, in another incident in 2023, the information of **80,000 Covid patients** was compromised when hackers paved their way into the Delhi State Health Mission's database. A hacking group from Kerala assumed responsibility for the attack and stated dissatisfaction with the government's handling of the pandemic as the reason for the breach.

Covid-19 information breach incident

2023

2020 and 2021

Justpay data leak

Impact: 35 Million Users

Justpay is an Indian payment portal utilized for making online payments. In 2020, unidentified actors hacked **35 million** user accounts of Justpay. A cyber-security expert confirmed the hacking in 2021 while surfing the dark web. According to him, the user data was being sold for 5000 dollars. The information on sale included card details and fingerprints of clients. The hackers were reportedly negotiating the prices via Telegram App due to its feature of timely self-erasure of stored information. Now that we have listed the top 7 data breaches of all time in India, let's look at some preventive measures that organizations can adopt to stay safe.

Journey So Far

2017

Hon'ble Supreme Court of India declared Right to Privacy as a fundamental right in K.S. Puttaswamy judgement

2018

Committee formed under the chairmanship of Justice Srikrishna submits report along with draft of PDP Act, 2018

2019

The PDP Act, 2019 introduced in the Lok Sabha and was referred to Joint Parliamentary Committee (JPC)

2021

JPC releases its report and a new version of the Act as Data Protection Act (DPA)

2022

Ministry of Electronics and Information Technology (MeitY) releases draft Digital Personal Data Protection Bill (DPDPB) for public consultation

2023

Union Cabinet approves the draft DPDP Bill, 2023

2023

The President of India assents to the Bill to make Digital Personal Data Protection (DPDP) an Act

Amendments to the Prevailing Law

Existing IT Act, 2000 and Right to Information Act 2005 are amended as following:

1. **Article 43(A) (Compensation for failure to protect data) of IT Act 2000 is omitted**

2. **Section 8 (1)(j) RTI Act 2005 is amended to exempt the personal information which allows disclosure for public interest.**

Applicability

Personal Data means "any data about any individual who is identifiable by or in relation to such data".

1. Private Companies
2. Partnership Firms
3. Public Companies
4. Foreign Companies
5. Government Entities
6. Other Body Corporates in India

Applicable to

Material Scope

- ✓ Personal Data that is **collected in digitized format**
- ✓ Personal Data that is collected in **non- digitized format and digitized subsequently.**

Territorial Scope

- ✓ Processing of personal data **within the territory of India**
- ✓ **Outside India** if activity related to offering goods and services to **Data principals within India**

Not Applicable to

- ✓ Processing for **domestic or personal** purposes by individuals.
- ✓ Personal data made **publicly available**.
- ✓ **Research Archiving and Statistics**.
- ✓ State Instrumentalities **– Sovereignty and Integrity of India.**

Commencement Timeline

While the Digital Personal Data Protection Act, 2023, is primed for implementation, the exact rollout date remains pending. The law's multifaceted nature necessitates a phased introduction, where distinct sections might come into effect at different junctures.

Key Stakeholders

1

Data Principal

An individual to whom the personal data relates; A child, includes the parents or lawful guardian of such a child; A person with disability, includes their lawful guardian acting on their behalf

2

Data Fiduciary

Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

3

Consent Manager

A consent manager represents the Data Principal and takes action on their behalf when granting, managing, reviewing and revoking consent.

4

Data Processor

Any person who processes personal data on behalf of a Data Fiduciary

Grounds of Processing of Data

Consent

The Data Principal may give, manage, review, or withdraw their consent to the Data Fiduciary directly or through the Consent Manager. **Privacy Notice to be provided at the time of obtaining consent.**

Consent Should be:

1. Freely Given
2. Specific
3. Informed
4. Unconditional
5. Unambiguous
6. Requires affirmation action

Legitimate Use

No Separate Consent is required for certain "**Legitimate Uses"** recognized under the Act. This includes where data is voluntarily provided or collected for a legal obligation**. Privacy Notice is not required for legitimate use.**

Legitimate Use

Legitimate Uses: Consent is not expressly needed for situations such as:

- Personal Data provided **voluntarily** by the Data Principal.
- Personal Data processed for any function under **any law or judgement issued under any law.**
- Responding to **medical emergency** involving a threat to the life of the Data Principal or other individual.
- Maintaining **public order and ensuring safety.**
- Purposes related to **employment.**
- Performing activities in **public interest.**

Obligations of Data Fiduciary

- Compliance with **DPDP Act**.
- Implement **technical and organizational measures** to ensure effective adherence with the Act.
- **Reasonable security safeguards** to prevent personal data breach.
- Engage with a **Data Processor** to process personal data on its behalf through a **valid contract only.**
- **Delete and erase data** as soon as the purpose is accomplished.
- **Report Personal Data Beaches** to Data Protection Board and Data Principals
- Provide a **clear, concise and comprehensible notice** to Data Principals
- Obtain **verifiable parental consent** before processing children’s personal data

Significant Data Fiduciary

Significant Data Fiduciary* will be determined based on an assessment which include

1. The **volume and sensitivity** of personal data processed
2. **Risk to the rights** of Data Principal
3. **Potential impact** on the sovereignty and integrity of India
4. **Risk to electoral** democracy
5. **Security of the state**
6. **Public order**

Obligations of the Significant Data Fiduciary

1. Appoint **a Data Protection Officer (DPO)** based in India
2. Appoint an **Independent Data Auditor** for evaluating compliance
3. Conduct **Data Protection Impact Assessment (DPIA)** & periodic audits

* Who will be the significant data fiduciary will be notified by the Government.

Rights & Obligations of Data Principal

1. **Right to access Information:** Data Principals have the right to seek information on how their data is processed, available in clear and understandable way.

2. **Right to Correction and Erasure:** Individuals have the right to correct inaccurate / incomplete data and erase data that is no longer required for processing

3. **Right to Nominate:** Individuals can nominate any other individual to exercise these rights in the event of death or incapacity

4. **Right to Grievance Redressal*:** Individuals have the right to readily available means of registering a grievance with a Data Fiduciary

5. **Right to Withdraw Consent:** Data principals have been empowered with the right to cease processing by withdrawing the consent.

Right to information, correction and erasure of personal data is applicable only where the grounds of processing is consent.

Obligations

They must not:

-register a **false or frivolous complaint,**

-furnish any **false particulars or impersonate another person in** specified cases.

Violation of duties will be punishable with a penalty of up to Rs 10,000.

**Timeline to respond to grievances raised by Data Principals shall be notified by the Central Government*

Cross- Boarder Transfer of Data

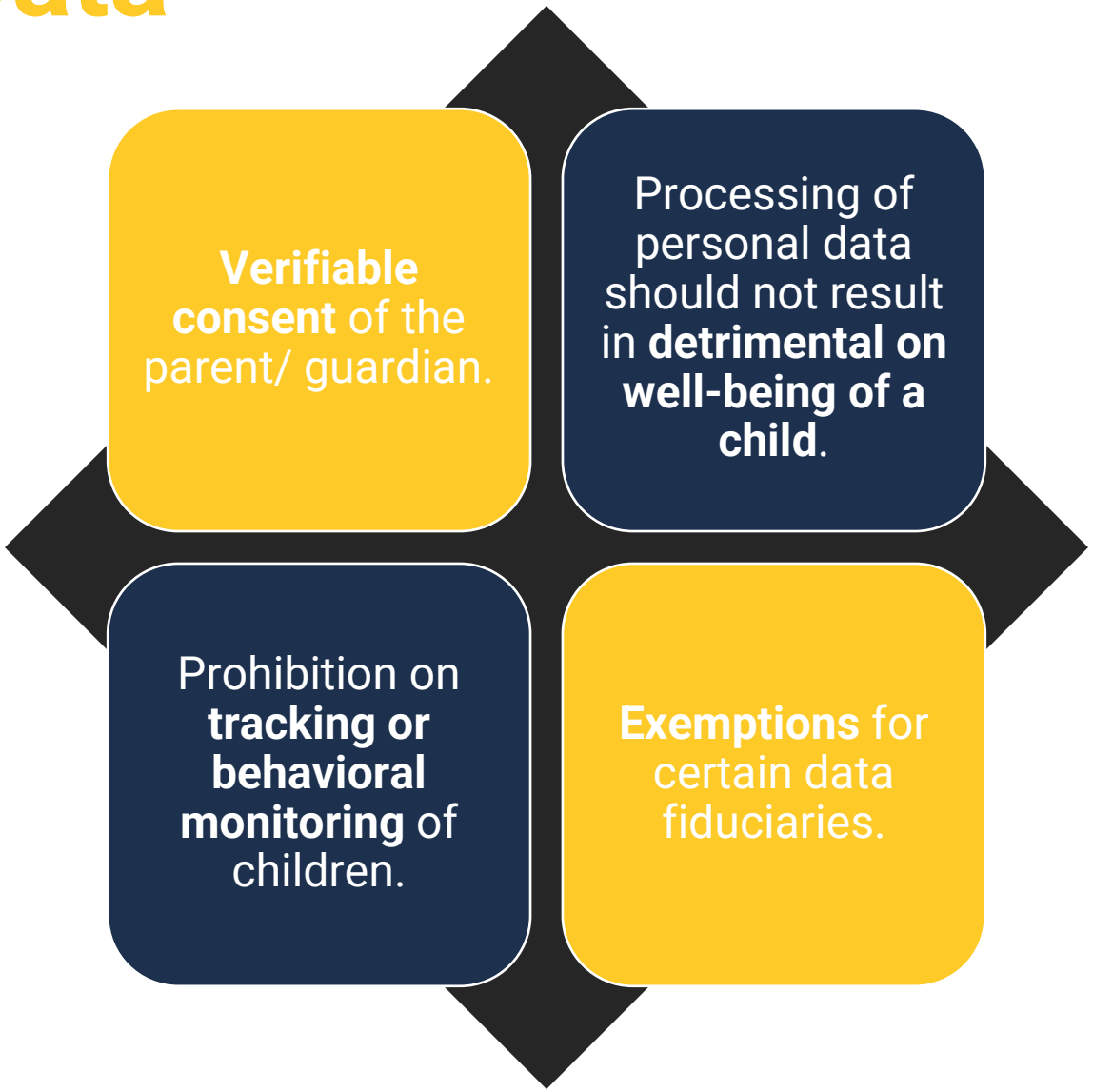
Consent of the data subject for transfer of Personal Data

Permitted unless restricted/ prohibited

Considerations

- ✓ Central Government may notify countries/ territories to which the transfers are **restricted/ prohibited.**
- ✓ **No clarity** on prospective implementation of this provision.
- ✓ No Clarity on **impact of existing personal data** hosted in such **restricted countries.**
- ✓ **Sectoral laws** which provide for higher degree of protection or restriction will prevail.

Children's Data



Other Features of the Act

- Considering the **volume and nature of personal data** processed, the Central Government may by notification exempt **certain provisions of the Act for a Data Fiduciary or a class of Data Fiduciaries** including startups

- When the consent for processing Personal Data was provided **before the commencement of this Act,** Data Fiduciary needs to provide detailed privacy notice describing the Personal Data collected and the purpose as soon as practicable after the enactment of this Act

- The Central Government may upon ensuring if the processing is verifiably safe, **notify the age above which a Data Fiduciary shall be exempt from applicability of children's personal data obligations**

- The Data Principal shall exhaust the opportunity of redressing her grievance with Data Fiduciary before approaching the Data Protection Board of India

Data Protection Board

The Central Government may, **by notification shall appoint** and establish, an independent board to be called the **Data Protection Board of India (Board).**

- ❑ This Board should consist of a **chairperson and other members**, who should be appointed by the Central Government.

- ❑ The Board is entrusted with the task of enforcement, including
  - ✓ determining non-compliances,
  - ✓ imposing penalties,
  - ✓ issuing directions and mediation (to resolve dispute between parties),
  - ✓ ensuring compliance with the law.

- ❑ The Board will have the power to hear **complaints against Consent Managers.**

- ❑ The Central Government will now have the power **to block a Data Fiduciary's platform.**

- ❑ Considering the **voluntary undertaking given by the data fiduciaries.**

- ❑ The Board is enshrined with powers of a civil court and appeals against its decisions lie to **Telecom Disputes Settlement and Appellate Tribunal**.

Penalties for Non-Compliance

The Data Protection Board has the power to issue **penalties up to INR 250 crore.**

Up to INR 250 Crore

Data fiduciaries are liable to pay a **penalty up to INR 250 crore** for a breach in observing the obligation of a **data fiduciary to take reasonable security safeguards to prevent personal data breach.**

INR 10,000

Penalty on **Data Principal** for breach in observance of the duties of a data principal shall lead to a penalty of INR 10,000.

Up to INR 200 Crore

Breach in observing the obligation to **give the board or affected data principal notice of a personal data breach** – non-Compliance in this case shall lead to a penalty **of INR 200 Crore.**

Breach in observance of additional obligations in relation to children- Non-compliance shall lead to a penalty of INR 200 Crore.

Up to INR 150 Crore

Breach in the observance of the additional obligations of a **significant data fiduciary-** non-compliance shall lead to a penalty of INR 150 crore.

INR 50 Crore

Breach of any other provisions of this act or the rules made thereunder- non-compliance shall lead to a penalty of INR 50 crores.

GDPR Vs DPDPA

General Data Protection Regulation (GDPR)	Digital Personal Data Protection (DPDP) Act, 2023
GDPR applies to processing of Personal Data wholly or partly by automated means and to Personal Data which form or will form a part of a filing system.	The DPDP Act will apply to digitized personal data and non-digitized personal data which is subsequently digitized
Penalties under GDPR extend **to 20 million euros, or 4% of the firm's** worldwide annual revenue from the preceding financial year, whichever amount is higher.	Penalties under the DPDP Act **extend up to INR 250 crore**
Minors **under age 16** need parental consent. Members states of Europe can lower this **age to 13** for their regions	Children under the **age of 18 need consent** from parents/ guardian
Breaches should be notified to the Supervisory Authority **within 72** hours and possibly to the affected Data Subjects	The Act does **not specify a timeframe** for Personal Data breach notification
GDPR **does not include right to nominate** however provides for the right to portability Organizations have 30 days to respond to a Data Subject request	The Act comprises of an **additional right to nominate** while omits the right to portability and timeline to respond to the Data Principal requests has not been specified
GDPR lays down specific mechanisms for **transferring data to third country** such as standard contractual clauses and binding corporate rules	The Act has **not identified any transfer mechanisms** for transferring Personal Data

GDPR Vs DPDPA

General Data Protection Regulation (GDPR)	Digital Personal Data Protection (DPDP) Act, 2023
Both Controllers and Processors are under the obligation to appoint **a DPO** in specific circumstance	**Only the Significant Data Fiduciary** shall have to appoint DPO as a point of contact for the Data Protection Board
Data Controller and Data Processor are required to maintain the records of processing activities (ROPA)	The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA)
GDPR **does not explicitly specify to provide notice to regional languages**	DPDP Act requires **the Data Fiduciaries to provide notice in 22 Indian languages in addition to English**
Data Protection Impact Assessment (DPIA) is to be conducted by Data Controllers for all the high-risk processing activities	**Significant Data Fiduciaries** are obligated to conduct periodic Data Protection Impact Assessment (DPIA)

Key Issues

The Bill does not regulate harm arising from processing of personal data

The Bill does not regulate risks of harms arising out of processing of personal data. The Srikrishna Committee (2018) had observed that harm is a possible consequence of personal data processing. Harm may include material losses such as financial loss and loss of access to benefits or services. It may also include identity theft, loss of reputation, discrimination, and unreasonable surveillance and profiling. It had recommended that harms should be regulated under a data protection law.

Shorter appointment term may impact independence of the Board

The Bill provides that members of the Data Protection Board of India will function as an independent body. Members will be appointed for two years and will be eligible for re-appointment. A short term with the scope for re-appointment may affect independent functioning of the Board.

Exemption from notice for consent may not be appropriate

The Bill empowers the central government to notify certain data fiduciaries or classes of data fiduciaries including startups from certain obligations.

Key Issues

Right to Data Portability and the Right to be Forgotten not provided

The Bill does not provide for the right to data portability and the right to be forgotten. The 2018 Draft Bill and the 2019 Bill introduced in Parliament provided for these rights. The Joint Parliamentary Committee, examining the 2019 Bill, recommended retaining these rights. GDPR also recognizes these rights. The Srikrishna Committee (2018) observed that a strong set of rights of data principals is an essential component of a data protection law. These rights are based on principles of autonomy, transparency, and accountability to give individuals control over their data.

Right to Data Portability: The right to data portability allows data principals to obtain and transfer their data from data fiduciary for their own use, in a structured, commonly used, and machine-readable format. It gives the data principal greater control over their data.

Right to be Forgotten: The right to be forgotten refers to the right of individuals to limit the disclosure of their personal data on the internet.

Key Issues

Adequacy of Protection in case of Cross-Border Transfer of Data

The Bill provides that the central government may restrict the transfer of personal data to certain countries through a notification. This implies the transfer of personal data to all other countries without any explicit restrictions

The aim of the regulation of transfer of personal data outside India is to safeguard the privacy of Indian citizens. In the absence of robust data protection laws in another country, data stored there may be more vulnerable to breaches or unauthorized sharing with foreign governments as well as private entities.

Exemptions to the State may have adverse Implications for Privacy

Personal data processing by the State has been given several exemptions under the Bill. As per Article 12 of the Constitution, the State includes: (i) central government, (ii) state government, (iii) local bodies, and (iv) authorities and companies set up by the government. There may be certain issues with such exemptions.

The Bill may enable unchecked data processing by the State, which may violate the right to privacy

Journey to Compliance

Assess the current Data Privacy posture, working practices and documentation against the requirement of DPDB

Data Privacy Assessment

Identify the Personal Data touch points and conduct data discovery and mapping activities

Data Discovery and Mapping

Identify the third- party ecosystem, ensure organizational and technical security measures are implemented through inclusion of the same within valid contracts

Third-Party Risk Management

Independent Data Privacy audits to identify the gaps and risks on a periodic basis

Internal Audit Assistance

Data Privacy Framework Development

Develop Data Privacy framework to strengthen your organization's data privacy program

Privacy Risk Assessment

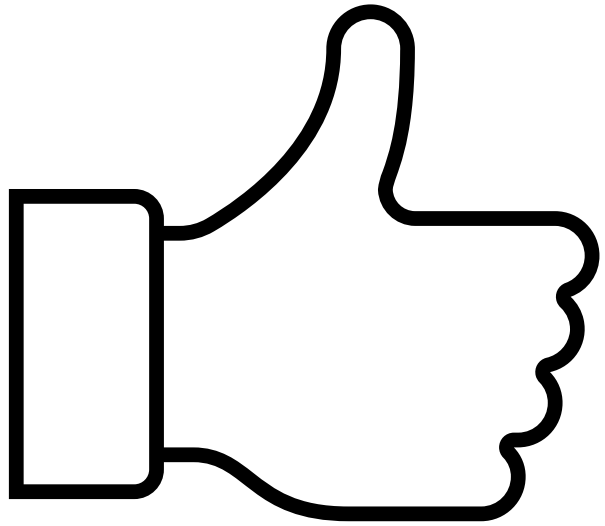
Perform Data Protection Impact Assessment (DPIA) for the high risk in scope business functions/ applications to identify the potential risk exposure

Privacy Enhancing Technologies

Reduce manual tasks with integrated workflow through Privacy Enhancing Technologies and manage your data governance activities in an automated manner

Training and Awareness

Socialization workshops for employees, management personnel and third parties to promote a privacy inclusive culture throughout the organization



Thanks!

email: divya@hrdco.in
Mob: +91-95825 72172