Introduction

The Ministry of Electronics and Information technology released the Digital Personal Data Protection Bill, 2022 on 18 November 2022. The bill seems to be a revamp of the older version. A data protection board will be set up for grievance redressal mechanisms and for imposing fines and penalties on data fiduciaries. The bill seems to be generic in nature as the keen ingredients like data localisation, cross-border data flow, free flow of data and right to be forgotten are not mentioned in their complete sense, thus creating a grey area for the execution of the said bill. The bill also imposes heavy penalties on data fiduciaries for non-compliance, however, the same seems harsh for start-ups and small business owners.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Introduction</td>
</tr>
<tr>
<td>II</td>
<td>Recommendations</td>
</tr>
<tr>
<td>III</td>
<td>Additional Suggestions</td>
</tr>
<tr>
<td>IV</td>
<td>Significance of the DPDP Bill, 2022</td>
</tr>
<tr>
<td>V</td>
<td>Way Ahead</td>
</tr>
<tr>
<td>VI</td>
<td>The differences between the Personal Data Protection Bill, 2019 &amp; Digital Personal Data Protection Bill, 2022</td>
</tr>
<tr>
<td>VI</td>
<td>Comparison between Digital Personal Data Privacy Bill, 2022 and General Data Protection Regulation, 2018</td>
</tr>
<tr>
<td>V</td>
<td>About CyberPeace Foundation</td>
</tr>
</tbody>
</table>
Section/Clauses: 2(3) & (6)

**Issues**: Rights of parents/guardians over data fiduciaries.

**Comments/Suggestions**: The child is protected by the consent of the parents/guardians but can a parent sue a data fiduciary in regard to involuntarily given data by a child?

Example - A child takes part in an online poll over social media and unknowingly gives out personal data, is the data fiduciary liable for such actions of the child?

**Rationale**: The rights, duties, and obligations of the parents need to be defined in order to prevent irrelevant and unnecessary cases in front of the board.

---

Section/Clauses: 4(1)(b)

**Issues**: Data localisation is generic in nature

**Comments/Suggestions**: The provision does not still the prime aspect of data localisation, i.e. to host data in our country. The aspect of cross-border data flow in the following provision provided an option for platforms to keep data out of physical reach from India.

**Rationale**: In case of a server located in the US, which hosts data of Indians is under attack by an enemy, who will hold the accountability for the Indian data in that server?

---

Section/Clauses: 4(3)(d)

**Issues**: The data of the older generation is not secure

**Comments/Suggestions**: Data older than 100 years is not recognized by the bill, but in case data is breached of an older generation or it's a matter of family inheritance will this bill recognise the digital rights of the older generations.

**Rationale**: The long-term effect of the act is restricted by this provision.
Section/Clause : 7

Issues : Scope of consent restricted

Comments/Suggestions : The consent for the corporate houses is not for the Government and it only recognises the provisions of this bill only.

Rationale : The aspect of consent has a large scope to it and hence the consent for the Government needs to be defined more clearly.

The flow of data from Corporate houses to the government and vice versa also needs to be addressed.

Section/Clause : 8 (2)

Issues : Unreasonable scope of access to data by Govt

Comments/Suggestions : The Govt does not need consent for data collection, thus is violative of Article 19(3).

Rationale : The government should set up steps and protocols for the consent of the netizen for data management or tracking.

Section/Clause : 8(5)

Issues : The apps like Aarogya Setu will be validated

Comments/Suggestions : The application launched in times of pandemic will have legal immunity to collect data, thus risking a breach of data by third-party actors.

Rationale : The restrictions and boundaries of data collection should be imposed in the bill to ensure no data is misused in times of a pandemic.
Section/Clause : 8(8)(b),(e),(f)& (g)

Issues : Unreasonable grounds of Public interest

Comments/Suggestions : The grounds of public interest are unreasonable to the public as well as the industry. The mentioned sub-sections have the following issues-
- 8(8)(b)- The aspect of Insolvency is absent
- 8(8)(e)- The operations of search engines bring a lot of uncertainty in terms of data tracking.
- 8(8)(f)- The publicly available data should be processed with the consent of the people.
- 8(8)(g)- How can recovery of debt be in the public interest as public banks or institutions are not mentioned in the bill?

Rationale : These provisions need to be amended and the real aspect of public interest needs to be incorporated into the same.

Section/Clause : 8 Illustration

Issues : How can Biometric data be shared?

Comments/Suggestions : Biometric data is a form of data that cannot be shared without the person. The illustration points towards data manipulation and tampering.

Rationale : The illustration needs to be removed and changed.

Section/Clause : 9(2)(b)

Issues : Data disclosed by one fiduciary to the other should be notified to the data principle

Comments/Suggestions : Sharing of data between two fiduciaries is an obligation of a data fiduciary and hence the data principles should be notified of any or all data exchanged.

Rationale : The provision needs a provision to implement the mandatory notifying of such data exchanges to users.
Section/Clause : 9(6)

Issues : Right to be forgotten

Comments/Suggestions : A specific time limit of the data expiration needs to be laid down as the same needs to be critically mentioned to prevent any bad actor from finding a loophole in the same.

Rationale : The Government should lay down time limits for different forms of data and highlight their expiration time.

Section/Clause : 11(1)(g)

Issues : The term electoral democracy imparts a negative influence on elections.

Comments/Suggestions : The term ‘risk of electoral elections’ needs to be removed and clearly defined in order to maintain the spirit of a free democracy.

Rationale : The provision needs to be removed and changed to bring the whole aspect of democracy under the domain of the bill.

Section/Clause : 13

Issues : The right to correction and erasure only for data fiduciaries.

Comments/Suggestions : The right to correction and erasure should not be enforced by data fiduciaries only. The same can be exercised by data principles as well.

Rationale : The option of auto-deletion or eraser of data should be made available for the data principle as well.
Section/Clause : 17

Issues : Cross-border data flow

Comments/Suggestions : The Govt needs to clearly highlight the aspects of cross-border data flow and the same should be kept under the transparency of the law rather than being with the power-centric central govt.

Rationale : The cross-border data flow should be defined in the definitions and the factors of the same should be enlisted in the bill.

Section/Clause : 21(13)

Issues : Powers of the board equivalent to a civil court

Comments/Suggestions : The power of the board should not be equivalent to the civil court as it will cause a lot of appeals to be filed at the high court. This is also in contradiction to sec 22(3) as no civil court can pass an order under this bill. How can the board be an independent body under the central govt exercising powers equivalent to a civil court.

Rationale : The board should rather set up a tribunal under the bill for timely and effective grievance redressal.

The board can also be declared to be a Quasi-Judicial Body.

Section/Clause : 22(2)

Issues : Time limit for appeal should be raised.

Comments/Suggestions : The period of limitation should be raised in order to allow a proper and unrushed investigation in case of appeal.

Rationale : The appeal period can be extended to 90 days to provide an adequate opportunity to the accused.
Section/Clause: 30(a),(c)

Issues: Compensation to the victims and powers of central govt.

Comments/Suggestions: The compensation to the victim is at the discretion of the board hence bringing ambiguity to the legal system.

The powers of the central Govt under the IT act have been increased and strengthened and the check on the power seems absent.

Rationale: The fine is paid to the boards and not to the data principal and hence the provision for compensation should be added to the bill. The powers of the central govt need to be under check to ensure proper separation of power.

Additional Suggestions

1. Opt-out Policy - The bill restricts the opt-out policy, if the user refuses the use of his data, he will lose the services as well. This is essentially a grey area and an advantage for platforms to transform and share user data with other fiduciaries.

2. Service Vendors - The service vendors will now establish practices that forcibly extract data from the users, thus violating privacy by and large.

3. Govt to Seek Consent - The government cannot collect data as per its desires and requirements and consent for any data collection must be sought from the netizen, this is a violation of Article 19(2) of the Constitution of India, which empowers only the parliament to enforce such laws.

4. Data Protection Board - The Data Protection Board should be established with a law passed by the parliament and the composition and the procedure of the same should be passed in the said law, thus creating transparency in the system.

5. Procedure for Insolvency - The bill needs to address the procedure and the criticalities for the insolvency procedures of a data fiduciary to prevent data breach and data monetizing by the fiduciary in case they treat their data as an asset.

6. High Penalties - The penalties are too high for small businesses and startups and hence these high penalties will also result in the withdrawal of major companies from India.
7. Data Differentiation - The Bill should classify data in terms of criticality and usage in order to implement the right to deletion and erasure more effectively which will prevent the bad actors from gaining access to data.

8. Data Localisation - The aspect of data localisation has been recognised partially, in real terms of data localisation, the fiduciaries should be encouraged to set up servers in India to ensure accountability and compliance with laws and policies, thus also creating employment opportunities as well.

9. Cross Border Data Flow - The bill lays down the provision for free flow of data with friendly nations, however the criteria for the same is absent and the indigenous data protection laws of a friendly nation should be taken into account for establishing data transfer with any nation. The Schrems judgement can be referred to, wherein the data transfer agreement was not allowed between the European Union & United States by the E.U Court of Justice due to inadequate data protection remedies for E.U citizens in case of breach by the US.

10. Data Insurance - The data fiduciaries should be made to create insurance for the data they host and store to protect the rights and interests of data principles.

11. VPN Policies - The use of VPN is not regulated in India, however, it is still seen to be a practice and is often the cause of data breaches, the bill can provide a consolidated stance on VPNs to eradicate any grey area in regard to the same.

12. Parental Monitoring Mode - The bill brings a child’s digital rights under the protection of his/her parents or guardians, the bill should also lay down mandates for data fiduciaries to create portals and applications where the parents/guardians can keep a check on the child’s online activity thus safeguarding them and also create a sense of accountability over the parents/guardians.

13. Data Tracking Under RTI - The data principal should have the privilege to file and Right To Information to keep a track of his or her data tracking and usage by fiduciaries.

14. Sandbox - The use of a sandbox to encourage innovation is critical and must be encouraged, however the same is absent from the current bill, thus creating a void for innovators and entrepreneurs.

15. Data Portability - The right to data portability allowed the data principal to receive in a structured format all the personal data they had provided to the data fiduciary and data that the data fiduciary generated on the data principal while processing for provisioning of its services.

16. Right to be Forgotten - Right to be Forgotten allows the data principal to ask the data fiduciary to stop the continuing disclosure of their personal data. The bill subsumes this right under the right to erasure conflation between the general right to erasure with the right to be forgotten which is specific to the disclosure of personal data, which compromises the right to freedom of speech and expression of other individuals.
17. **Scope of Compliance** - The bill lays down heavy penalties but the same seems to be a shield for the corporate houses, as per the bill, the only effective remedy of data or consent breach by the fiduciaries is fine hence creating a scope of the vulnerability of the data principles.

18. **Inflow of Data from Other Countries** - The bill needs to highlight the SoPs for data coming in the country as various Indian tech companies are processing foreign data.

19. **Exhaustive List** - Companies to lose business in case of an exhaustive list of friendly nations.

20. **Softcopy or Hardcopy Breach** - The bill needs to clearly highlight the classification of data and its breach, in case data is converted into hard copy and then circulated with wrong intentions, will it be covered under the bill?

21. **Data Printout** - The bill highlights the aspects of data types, being in digital form, but would a physical copy of the said data be covered under the bill?

22. **Incident reporting** - The bill also needs to highlight the timelines for incident reporting to encourage timely reporting.

23. **‘Individual’ to ‘Person’** - It is suggested to change the term “Individual” to “Person” to remove ambiguity regarding the identity of Data Fiduciary and Data Principle.

24. **Privacy Title** - Since the bill is focusing on the data privacy of data principle, the term “Privacy” should be added to the Long and the Short title of the bill.

25. **DP Commission** - A data Protection Commission should be set up in order to maintain transparency and check on the powers of the Central Govt.

**Significance of the DPDP Bill, 2022**

- Strong safeguards, as fines for data misuse prescribed in the previous version of the Bill were not seen as an effective deterrent.
- The higher penalties being proposed now will prompt entities to build strong safeguards to protect data and enforce fiduciary discipline.
- Companies would face punitive actions in the nature of financial penalties in the event of misuse of data and data breaches.
- The upcoming data protection Bill will put an end to the misuse of customer data with companies facing financial consequences.
- There will also be a strict or purpose limitation of data collected by companies and the time till which they can store it under the new Bill.
- Data fiduciaries will be required to stop retaining personal data and delete previously collected data after the initial purpose for which it was collected was fulfilled.
Way Ahead

- While protecting the rights of the data principal, data protection laws need to ensure that the compliances for data fiduciaries are not so onerous as to make even legitimate processing impractical.

- The challenge lies in finding an adequate balance between the right to privacy of data principles and reasonable exceptions, especially where government processing of personal data is concerned.

- Given the rate at which technology evolves, an optimum data protection law design needs to be future-proof — it should not be unduly detailed and centred on providing solutions to contemporary concerns while ignoring problems that may emerge going forward.

- The law needs to be designed for a framework of rights and remedies that is readily exercisable by data principals given their unequal bargaining power with respect to data fiduciaries.
The differences between the Personal Data Protection Bill, 2019 & Digital Personal Data Protection Bill, 2022

Parameter: Personal Data

**PDP, 2019**: Only excluded data processed manually specifically by small entities

**DPDP, 2022**: Completely inapplicable to data processed manually

**Remarks**: The new Bill provides a lower degree of protection

Parameter: Data Localisation

**PDP, 2019**: Mandated enterprises to keep a copy of sensitive personal data within India and prohibited the transfer of critical personal data from the country

**DPDP, 2022**: Relaxes data localisation rules and permits data to flow to certain global destinations, based on their data security landscape

**Remarks**: The new Bill made the changes to address the concerns expressed by IT firms

Parameter: Regulation of social media and non-personal data

**PDP, 2019**: Included

**DPDP, 2022**: Drops provisions to regulate non-personal data (information that does not reveal the identity of an individual) and social media

**Remarks**:
Parameter : The right to post-mortem privacy

PDP, 2019 : No such provision

DPDP, 2022 : Included

Remarks : It would allow the data principal (users) to nominate another individual in case of death or incapacity

Parameter : Territorial application of the law

PDP, 2019 : Included

DPDP, 2022 : Excludes data processing by Indian data fiduciaries that collect and process personal data outside India, of data principals who are not located in India

Remarks : Impact statutory protections available for clients of Indian start-ups operating overseas, thus impacting their competitiveness

Parameter : Penalty

PDP, 2019 : Criminal conviction

DPDP, 2022 : The focus is more on financial penalties

Remarks : –

Parameter : Personal Sensitive Data

PDP, 2019 : The term personal sensitive data has been well defined.

DPDP, 2022 : The term is not provided under the definitions or any provision

Remarks : The term needs to be defined in order to secure the digital rights of the netizens.
Parameter: Crime Against children

PDP, 2019: Provisions were well defined.

DPDP, 2022: Criminal procedure and provisions missing from the bill.

Remarks: Crimes against activities need to be given legal recognition to protect the interest of their children.

Parameter: Innovation

PDP, 2019: Sandbox was mandated and defined

DPDP, 2022: Sandbox is not mentioned in the bill.

Remarks: Innovative practices will be substantiated with govt regulated Sandbox.

Parameter: Appellate Tribunal

PDP, 2019: Provision laid down

DPDP, 2022: No provision regarding a tribunal

Remarks: All matters will be taken up by the board, however establishing a tribunal like the telecommunication tribunal will go a long way to reduce the number of pending cases.
Comparison between Digital Personal Data Privacy Bill, 2022 and General Data Protection Regulation, 2018

<table>
<thead>
<tr>
<th>Parameter</th>
<th>GDPR, 2018</th>
<th>DPDP, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categorization of Data</td>
<td>GDPR has a classification of data as personal data and, along with it, there are other classifications of data as ‘special categories’ which include data such as those relating to racial/ethnic origin, political opinions, trade union membership, and the processing of genetic data.</td>
<td>DPDP Bill has classified certain data as personal data, which are to be regulated, and there exist no other classifications like sensitive or special personal data which existed in the previous iterations of the bill.</td>
</tr>
<tr>
<td>Processing of Children’s Data</td>
<td>GDPR has adopted a graded approach for permissions required for the processing of personal data of children. The age for valid consent ranges in such cases ranges from 13 to 16 years depending on the Member States.</td>
<td>DPDP, 2022 lays down a child to be an individual under the age of 18 years. The bill mentions that in case parental consent is obtained by the entity for processing data of children, it is deemed consent.</td>
</tr>
<tr>
<td>Fundamental Principles Guiding Processing of Personal Data</td>
<td>GDPR clearly mentions under Article 5 that Lawfulness, Fairness &amp; Transparency, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity &amp; Confidentiality, and Accountability shall be the core principles guiding the processing of personal data.</td>
<td>The DPDP Bill has no express mention of any such principles.</td>
</tr>
</tbody>
</table>
Parameter: Cross Border Flow of Data

**GDPR, 2018**: GDPR under Chapter 5 has laid down an exhaustive procedure for cross border flow of data. This is implemented through adequacy decisions, prescribed rules, standard contracts, and clauses relating to derogation.

**DPDP, 2022**: DPDP Bill, on the other hand, has dealt with the idea of cross border flow of data in a fleeting and open-ended manner. The transfer of personal data has been allowed ‘freely’ to ‘trusted’ jurisdictions which are to be notified at a later stage.

Parameter: Introduction of Consent Managers

**GDPR, 2018**: No such provision in GDPR

**DPDP, 2022**: DPDP Bill has introduced the involvement of third-party ‘consent managers’ who would serve as a link between the data principal and the data fiduciary.

Parameter: Data Breach Notification

**GDPR, 2018**: GDPR mandates reporting of data breaches to data principals only in cases when a personal data breach is likely to result in significant harm to the rights and freedoms of data subjects.

**DPDP, 2022**: DPDP Bill takes a more stringent approach by mandating the reporting of all kinds of data breaches to data principals, irrespective of their effects.

Parameter: Penalties on Non-Compliance

**GDPR, 2018**: GDPR prescribes fines under Article 83 and the same are administered according to the size of the organisation, gravity, and impact on non-compliance, and other criteria.

**DPDP, 2022**: The DPDP Bill prescribed an upper limit on the financial penalty for non-compliance and the same has been limited to not more than INR 500 crores.
CyberPeace Foundation (CPF) is a global civil society organization, think tank of cybersecurity and policy experts with the vision of pioneering CyberPeace Initiatives to build collective resiliency against cybercrimes and global threats of cyber warfare. CPF is involved in Policy Advocacy, Research and Training related to all aspects of CyberPeace and Cyber Security. Key areas of CyberPeace Foundation's work are in Technology Governance, Policy Review and Advocacy, Capacity and Capability creation and building through partnerships with various government organizations, academic institutions and civil society entities.

MISSION
To work with netizens, national and international institutions to facilitate inclusion, security, stability and trust.

VISION
Peaceful, Responsible and Inclusive Cyber Space
CyberPeace Foundation’s work towards Internet Governance and Cyber Security is aligned towards 6 UN’s Sustainable Development Goals (SDGs).

Verticals of #CyberPeace

Policy Advocacy & Cyber Diplomacy

Innovation & Research

Inclusion & Outreach

Collaboration & Connect

Impacted 200 Million netizens across 112 countries!

CyberPeace Revolution has taken the globe by storm!