

**48**

**STANDING COMMITTEE ON  
COMMUNICATIONS AND  
INFORMATION TECHNOLOGY  
(2022-23)**

**SEVENTEENTH LOK SABHA**

**MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY**

**CITIZENS' DATA SECURITY AND PRIVACY**

**FORTY-EIGHTH REPORT**



**LOK SABHA SECRETARIAT  
NEW DELHI**

*August, 2023/ Sravana, 1945 (Saka)*

**FORTY- EIGHTH REPORT**

**STANDING COMMITTEE ON  
COMMUNICATIONS AND  
INFORMATION TECHNOLOGY  
(2022-23)**

**(SEVENTEENTH LOK SABHA)**

**MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY**

**CITIZENS' DATA SECURITY AND PRIVACY**

*Presented to Lok Sabha on 1 August, 2023*

*Laid in Rajya Sabha on 1 August, 2023*



**LOK SABHA SECRETARIAT**

**NEW DELHI**

*August, 2023/ Sravana, 1945 (Saka)*

<b>CONTENTS</b>		
		<b>Pg. No.</b>
	COMPOSITION OF THE COMMITTEE (2019-20)	
	COMPOSITION OF THE COMMITTEE (2020-21)	
	COMPOSITION OF THE COMMITTEE (2021-22)	
	COMPOSITION OF THE COMMITTEE (2022-23)	
	INTRODUCTION	
	<b>REPORT</b>	
	<b>PART-I</b>	
1.	Introductory- Need for Dedicated Legislation on Data Privacy	
2.	The Cyber Conundrum- Addressing the surge of cyber crimes and urgent call for regulatory action	
3.	Inclusive and Comprehensive Consultation Journey for Comprehensive Solutions	
4.	Globally Aligned Bill- Embracing International Best Practices	
5.	Unleashing the Digital India Bill	
6.	Need for amendments in IT Act	
7.	Ensuring Robust Safeguards Within the Bill For Inclusive Digital Access	
8.	Enhancing Citizen Awareness and Safeguarding Digital Personal Data	
9.	Significance of Consent in the Draft Bill	
10.	Certain exemptions (Legitimate Uses) to Maintain Public Order	
11.	Accountability and Deterrence Mechanism under the Digital Personal Data Protection Bill	
12.	Flexibility and evolvability of the provisions of the draft Bill	
	<b>PART-II</b>	
	OBSERVATIONS/RECOMMENDATIONS	
	<b>ANNEXURES</b>	
I.	Draft Digital Personal Data Protection Bill, 2022	
II.	Dissent Note submitted by Dr. John Brittas, MP (Rajya Sabha)	
	<b>APPENDICES</b>	
I.	Minutes of the Fourth Sitting of the Committee held on 02.12.2022	
II.	Minutes of the Fifteenth Sitting of the Committee held on 15.06.2023	
III.	Minutes of the Sixteenth Sitting of the Committee held on 26.07.2023	

## COMPOSITION OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2019-20)

**Dr. Shashi Tharoor - Chairperson**

### **Lok Sabha**

2. Smt. Locket Chatterjee
3. Shri Karti P. Chidambaram
4. Shri Sunny Deol
5. Dr. Nishikant Dubey
6. Shri Vijay Kumar Dubey
7. Choudhary Mehboob Ali Kaiser
8. Smt. Raksha Nikhil Khadse
9. Dr. Sukanta Majumdar
10. Shri Dhairyasheel Sambhajirao Mane
11. Ms. Mahua Moitra
12. Shri P. R. Natarajan
13. Shri Santosh Pandey
14. Shri Nisith Pramanik
15. Col. Rajyavardhan Singh Rathore
16. Dr. Gaddam Ranjith Reddy
17. Shri M V V Satyanarayana
18. Shri Sanjay Seth
19. Shri L.S. Tejasvi Surya
20. Dr. T. Sumathy (A) Thamizhachi Thangapandian
21. Shri Bhanu Pratap Singh Verma

### **Rajya Sabha**

22. Dr. Anil Agrawal
23. Dr. Subhash Chandra
24. Shri Y. S. Chowdary
25. Shri Suresh Gopi
26. Shri Md. Nadimul Haque
27. Shri Syed Nasir Hussain
28. Dr. Narendra Jadhav
29. Shri Shaktisinh Gohil\*
30. Shri Parimal Nathwani\*
31. **VACANT**#

---

Committee constituted w.e.f. 13<sup>th</sup> September, 2019 *vide* Bulletin Part-II Para No. 542 dated 13<sup>th</sup> September, 2019.

\* Nominated to the Committee w.e.f. 22nd July , 2020 *vide* Para No.1370 Bulletin Part-II dated 24 July, 2020

# Shri Beni Prasad Verma, MP, Rajya Sabha, expired on 27th March, 2020.

**COMPOSITION OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY**  
**(2020-21)**

**Dr. Shashi Tharoor - Chairperson**

**Lok Sabha**

2. Smt. Locket Chatterjee
3. Shri Karti P. Chidambaram
4. Dr. Nishikant Dubey
5. Smt. Sunita Duggal\*
6. Smt. Raksha Nikhil Khadse
7. Dr. Sukanta Majumdar
8. Shri Dhairyasheel Sambhajirao Mane
9. Ms. Mahua Moitra
10. Shri P. R. Natarajan
11. Shri Santosh Pandey
12. Col. Rajyavardhan Singh Rathore
13. Dr. Gaddam Ranjith Reddy
14. Shri Jayadev Galla
15. Shri Sanjay Seth
16. Shri Chandan Singh
17. Shri L.S. Tejasvi Surya
18. Dr. T. Sumathy (A) Thamizhachi Thangapandian
19. Smt. Sumalatha Ambareesh
20. Shri Ganesh Singh\*
21. Shri Parvesh Sahib Singh\*

**Rajya Sabha**

22. Dr. Anil Agrawal
23. Dr. Subhash Chandra
24. Shri Y. S. Chowdary
25. Shri Shaktisinh Gohil
26. Shri Suresh Gopi
27. Shri Md. Nadimul Haque
28. Shri Syed Nasir Hussain
29. Shri Syed Zafar Islam
30. Dr. Narendra Jadhav
31. Shri Nabam Rebia

---

\* Smt. Sunita Duggal, Shri Ganesh Singh and Shri Parvesh Sahib Singh (vice Shri Sunny Deol) were nominated to the Committee vide Para No. 2822 of Bulletin Part-II dated 27 July, 2021.

**COMPOSITION OF THE STANDING COMMITTEE ON COMMUNICATIONS AND  
INFORMATION TECHNOLOGY (2021-22)**

**Dr. Shashi Tharoor - Chairperson**

**Lok Sabha**

2. Smt. Sumalatha Ambareesh
3. Smt. Locket Chatterjee
4. Shri Karti P. Chidambaram
5. Dr. Nishikant Dubey
6. Smt. Sunita Duggal
7. Shri Jayadev Galla
8. Smt. Raksha Nikhil Khadse
9. Dr. Sukanta Majumdar
10. Shri Dhairyasheel Sambhajirao Mane
11. Ms. Mahua Moitra
12. Shri Santosh Pandey
13. Shri P. R. Natarajan
14. Col. Rajyavardhan Rathore
15. Dr. Gaddam Ranjith Reddy
16. Shri Sanjay Seth
17. Shri Ganesh Singh
18. Shri Parvesh Sahib Singh
19. Shri Tejasvi Surya
20. Dr. T. Sumathy (A) Thamizhachi Thangapandian
21. **Vacant**

**Rajya Sabha**

22. Dr. Anil Agrawal
23. Shri John Brittas
24. Dr. Subhash Chandra
25. Shri Y. S. Chowdary
26. Shri Ranjan Gogoi
27. Shri Suresh Gopi
28. Shri Syed Nasir Hussain
29. Shri Syed Zafar Islam
30. Shri Jawhar Sircar
31. **Vacant**

---

Committee constituted w.e.f. 13 September, 2021 *vide* Para No.3184 of Bulletin Part-II dated 9 October, 2021.

**Composition of the Standing Committee on Communications and  
Information Technology (2022-23)**

**Shri Prataprao Jadhav - Chairperson**

**Lok Sabha**

2. Smt. Sumalatha Ambareesh
3. Shri Karti P. Chidambaram
4. Dr. Nishikant Dubey
5. Smt. Sunita Duggal
6. Shri Jayadev Galla
7. Smt. Raksha Nikhil Khadse
8. Dr. Sukanta Majumdar
9. Smt. Mahua Moitra
10. Shri P. R. Natarajan
11. Shri Santosh Pandey
12. Col. Rajyavardhan Singh Rathore
13. Dr. Gaddam Ranjith Reddy
14. Shri Sanjay Seth
15. Shri Ganesh Singh
16. Shri Parvesh Sahib Singh
17. Shri Shatrughan Prasad Sinha
18. Shri L.S. Tejasvi Surya
19. Dr. T. Sumathy (A) Thamizhachi Thangapandian
20. Dr. M. K. Vishnu Prasad
21. Shri S. Jagathrakshakan

**Rajya Sabha**

22. Dr. Anil Agrawal
23. Shri V. Vijayendra Prasad
24. Dr. John Brittas
25. Shri Syed Nasir Hussain
26. Shri Ilaiyaraaja
27. Shri Jaggesh
28. Shri Praful Patel
29. Shri Kartikeya Sharma
30. Shri Jawhar Sircar
31. Shri Lahar Singh Siroya

**Secretariat**

- |                       |   |                   |
|-----------------------|---|-------------------|
| 1. Shri Satpal Gulati | - | Joint Secretary   |
| 2. Shri Nishant Mehra | - | Deputy Secretary  |
| 3. Smt. Rinku Awasthi | - | Executive Officer |

---

Committee constituted w.e.f. 13<sup>th</sup> September, 2022 *vide* Para No.5288 of Bulletin Part-II dated 4<sup>th</sup> October, 2022.

## **INTRODUCTION**

I, the Chairperson, Standing Committee on Communications and Information Technology (2022-23), having been authorized by the Committee do present the Forty-eighth Report on the subject 'Citizens' Data Security and Privacy' relating to the Ministry of Electronics and Information Technology.

2. The erstwhile Standing Committee on Information Technology (2019-20) selected this subject for detailed examination and Report to the Parliament. The examination of the Subject, however, could not be completed during the term of the Committee (2020-21). Keeping in view the importance of the subject and the need for wider consultation, the Committee re-selected the subject during its terms 2020-21, 2021-22 and 2022-23.

3. During the term 2019-20, the representatives of the Ministry of Electronics and IT, Ministry of Home Affairs and Department of Atomic Energy gave evidence before the Committee on the subject on 20 November, 2019. Thereafter, cyber security experts, non-official witnesses, representatives of Whatsapp and Dept of Telecommunications, Ministry of Home Affairs and Chief Secretary, Govt. of NCT of Delhi gave evidence on 13 December, 2019. During 2020-21, no Sittings were held on the Subject. During 2021-22, three Sittings were held on 26 August, 2022 on which representatives of Twitter India, Fairwork India and IRCTC were called for evidence. During 2022-23, the representatives of the Ministry of Electronics and Information Technology gave evidence before the Committee on the subject on 2 December, 2022 and 15 June, 2023. A dissent note submitted by Dr. John Brittas, M.P. ( Rajya Sabha) is appended to the Report.

4. The Committee at their Sitting held on 26 July, 2023 considered and adopted the Report. The Committee wish to express their thanks to the representatives of the Ministries/Departments and experts/witnesses of private entities who tendered evidence during its Sittings.

5. The Committee also place on record their appreciation for the invaluable assistance rendered by the officials of Lok Sabha Secretariat attached to the Committee.

6. For facility of reference and convenience the Observations/Recommendations of the Committee have been printed in bold in Part-II of the Report.

**New Delhi;**  
**31 July, 2023**  
**9.Sravana, 1945 (Saka)**

**PRATAPRAO JADHAV,**  
**Chairperson,**  
**Standing Committee on**  
**Communications and Information Technology.**



## **PART-I REPORT**

### **I. Introductory- Need for Dedicated Legislation on Data Privacy**

1. Personal data security and privacy issues have figured predominately in public discussion and debate in recent years. The Supreme Court of India, in a judgement delivered by a nine-judge bench in 2017, has held that the right to privacy is protected as part of the fundamental rights guaranteed by the Constitution of India. Digital India has caused digitisation of the Indian economy and transformed the lives of Indian citizens in particular and governance in general. The lives of crores of Indians and their experience of governance have been significantly enhanced by the use of technology and the Internet. Digital India has also unleashed innovation and entrepreneurship in the digital space in addition to the large global Big Tech platforms that have significant presence on the Internet.
2. Presently, there are over 80 crore Internet users. India is the largest connected democracy in the world and is amongst the highest consumers and producers of data per capita amongst the countries. It has become clear over the last few years that while the Internet and technology are a force for good and connectivity, Internet is also a place where user harm and misuse can exist if rules and laws are not prescribed. That is why laws and rule-making for the Internet has to be around the basic foundational principles and expectations of the citizens of openness, safety and trust and accountability.
3. Data in general and personal data in specific are at the core of this fast-growing digital economy and ecosystem of digital products, services and intermediation. It has become very clear over the last few years whilst this data is used by platforms and intermediaries, the data and personal data must be subject to a framework of rules and dos and don'ts. To sum up, while digitisation using personal data of Data Principals has transformed delivery of services to them enhancing ease of living, Data Principals are also increasingly at risk of harm from misuse of their personal data. Further, the Supreme Court, in its judgement in the Puttaswamy case in 2017, has declared the right to privacy as protected as part of the fundamental rights guaranteed by the Constitution. Therefore, it has become imperative that digitised personal data be protected. At the same time, it is necessary to ensure that Data Principals in India benefit from the innovation ecosystem of Digital India for continuous improvement in delivery of services and enhancement of ease of living, and the digital economy continues to grow with economic benefits for all. With this in view, Government published for public consultation a draft Bill titled "the Digital Personal Data Protection Bill, 2022"( Annexure-I), which casts obligations on Data

Fiduciaries for protection of personal data and makes them accountable for the same, and provides for the rights and duties of Data Principals.

4. The Bill seeks to enhance Ease of Living and Ease of Doing Business in the following ways:

### **Highlights of the Data Bill:**

#### *Aims*

- The proposed Bill seeks to achieve the following:
  - (a) Introduce data protection law with minimum disruption while ensuring necessary change in the way Data Fiduciaries process data;
  - (b) Enhance the Ease of Living and the Ease of Doing Business; and
  - (c) Enable India's digital economy and its innovation ecosystem.

#### *Approach and principles*

- The proposed Bill seeks to provide for the use of personal data by platforms, intermediaries and other Data Fiduciaries or Data Processors subject to a framework of rules and do's and don'ts. It is based on the following principles, which have formed the basis for personal data protection laws in various jurisdictions:
  - (a) The principle that usage of personal data by organisations must be done in a lawful manner, which is fair and transparent to the Data Principals;
  - (b) The principle of purpose, *i.e.*, the personal data be used only for the purpose for which it was collected;
  - (c) The principle of data minimisation, *i.e.*, only those items of personal data be collected as are required for attaining the specified purpose;
  - (d) The principle of accuracy of personal data, *i.e.*, reasonable effort be made to ensure that the personal data is accurate and kept up to date;
  - (e) The principle of storage limitation, *i.e.*, personal data not be stored perpetually by default and storage be limited to such duration as is necessary for the specified purpose;
  - (f) The principle that reasonable safeguards be taken to prevent personal data breach; and
  - (g) The principle that the person who decides the purpose and means of processing of personal data should be accountable for such processing.

#### *Minimising disruption*

- The proposed Bill seeks to minimise disruption through provision for the following:
  - (a) Allowing for continuing validity of processing based on pre-existing consent (unless withdrawn), while requiring Data Fiduciary to notify the Data Principal;

- (b) Making provision for consistency with sectoral laws, so that the basic protection is ensured under the Bill while additional regulation/protection may continue to be applicable under sector-specific law; and
- (c) Enabling processing outside India, while retaining India's right to restrict processing in notified countries.

#### *Ease of Living and Ease of Doing Business*

- The Bill seeks to enhance Ease of Living and Ease of Doing Business in the following ways:
  - (a) By laying down the principles to be followed by Data Fiduciaries to protect personal data, while avoiding a prescriptive approach and intrusive regulation;
  - (b) By providing for the first time a fully digital-by-design online complaint resolution mechanism through the Data Protection Board, which will function as a digital office whose entire proceedings, from their institution till disposal, are in online or digital mode;
  - (c) By enabling faster resolution by the Board by providing for the referring of matters for Alternate Dispute Resolution through a mediator identified by the parties and the acceptance of Voluntary Undertakings from Data Fiduciaries;
  - (d) Not providing for criminalisation of breaches, while providing for deterrent financial penalties for breach in observance of the Bill's provisions; and
  - (e) By providing for user to get the notice seeking his/her consent in any of the Indian languages listed in the Eighth Schedule to the Constitution.

#### *Concise and SARAL*

- The proposed Bill is concise and **SARAL**, that is, **S**imple, **A**ccessible, **R**ational & **A**ctionable **L**aw. It uses plain language, contains illustrations that make the meaning clear, contains no provisos ("provided that...") and has minimal cross-referencing.
- By using the word "she" instead of "he", for the first time women are being acknowledged in law-making by the Indian Parliament.

#### *Other innovative aspects*

- The proposed Bill, while retaining the core principles of data protection in the earlier Bill (notice for collecting or processing personal data, consent, purpose and storage limitation, accuracy of data, etc.), offers a simpler law which is easy to understand and administer. Examples of this include the following:
  - (a) There is no classification of personal data, which is sought to be protected as a whole, thereby avoiding issues of interpretation and classification-based protection.

- (b) In addition to the rights under the earlier Bill, the proposed Bill also includes the right to nominate a person to exercise rights in the event of death or incapacity of the Data Principal. Further, associated are duties entrusted to an individual.
- (c) It defines the obligations of Data Fiduciaries and fixes accountability for breach in their observance without adding to compliance burden.

### **Highlights of key provisions of the Data Bill:**

- The provisions of the Bill as published have been revisited in light of feedback received from the public, stakeholders and Ministries/Departments. Broad highlights of key aspects of the Bill are summarised in the succeeding paragraphs.

#### *Applicability*

- The provisions of the Bill would apply to personal data collected in digital form or collected in non-digital form and digitised subsequently in India, as well as to personal data processed outside India for offering goods and services in India. It would not be applicable to personal data processed for personal or domestic purpose, personal data made publicly available by the Data Principal or by any other person pursuant to a legal obligation.

#### *Basis of data processing*

- The following would constitute the basis of data processing under the Bill:
  - (a) Processing may be done only in accordance with the provisions of the Bill and the rules made thereunder;
  - (b) It may be done only for lawful purposes; and
  - (c) It may be done on consent, or for certain legitimate uses specified in the Bill.

#### *Consent*

- Before requesting consent, the Data Fiduciary must give a notice specifying the purpose for which data will be processed, with the option to access it in any of the Indian languages listed in the 8<sup>th</sup> Schedule to the Constitution. Consent given shall be limited to personal data necessary for such purpose, and the giving of consent for personal data not necessary for the purpose may not be made a condition for processing. It shall be withdrawable at any time.
- Consent Managers accountable to the Data Principal may serve as single points of contact to enable them to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform.
  - To avoid disruption, where the Data Principal has given consent before the proposed enactment, the Data Fiduciary shall be obligated to give notice regarding the same to the Data Principal, while continuing to process the data, unless consent is withdrawn.

### *Certain legitimate uses*

- Taking into account the feedback received, processing of personal data for certain legitimate uses is now proposed to be more focussed than in the draft published for public consultation. Broadly, such uses would include performance by the State and its instrumentalities of functions under law, or in the interest of sovereignty, integrity and security of the State, or for providing/issuing subsidies, benefits, services, certificates, licences and permits prescribed by rules. They would also include disclosures for fulfilling any obligation under law, compliance with any judgement or order under law, protection/assistance/service in a health emergency, disaster or public order situation, and in relation to employees.

### *Obligations of Data Fiduciary*

- Broadly, the proposed obligations of the Data Fiduciary will include implementation of technical and organisational measures for compliance, security safeguards to prevent data breach, intimation of data breaches to affected Data Principals and the Data Protection Board, erasure of data upon withdrawal of consent or when retention is no longer necessary for the specified purpose, publishing of contact details of person to answer queries of Data Principals, establishing of a grievance redressal system, and use of Data Processors only under contract.
- Further, certain additional obligations are proposed in respect of Data Fiduciaries notified as Significant Data Fiduciaries, such as appointing a data auditor and conducting periodic Data Protection Impact Assessment to ensure higher degree of data protection.

### *Safeguards for processing of children's data*

- Broadly, the safeguards proposed for processing of personal data of children include processing only with parental consent and not undertaking processing detrimental to children's well-being or involving tracking, behavioural monitoring or targeted advertising. However, to enable use in cases like protection of abandoned children, etc., Government may notify purposes where processing may be allowed without parental consent or with tracking etc.

### *Rights of Data Principals*

- The rights of the Data Principals are the right to access information about personal data processed, the right to correction and erasure of data, the right to grievance redressal and the right to nominate a person to exercise rights in case of death or incapacity. For enforcing the rights, the affected Data Principal may approach the Data Fiduciary through its grievance redressal mechanism and, if not satisfied, complain online to the Data Protection Board.

### *Duties of Data Principals*

- The proposed duties are aimed at ensuring the reliability of personal data used in data processing. Broadly, the duties proposed include compliance with applicable laws, not impersonating while providing data, not suppressing material information while providing any document or identity/address proof, not making false or frivolous grievance/complaint and giving only verifiably authentic information while using the right to correct or erase data.

### *Processing outside India*

- The provisions of the Bill in this regard have been revisited in the light of the feedback received. Broadly, it is now proposed to allow processing of personal data outside India unless the Government notifies any country or territory for which processing shall be restricted.

### *Exemptions*

- The provisions regarding exemptions have also been revisited in light of the feedback and, broadly, the exemptions now proposed include processing by the State and its notified instrumentalities in the interests of sovereignty, integrity, security of the State, friendly foreign relations, public order or incitement of related offence. They also include processing for research, archiving or statistical purposes, for startups or other notified categories of Data Fiduciaries, for enforcement of legal rights and claims, for performance of judicial or regulatory functions, for preventing, detecting, investigating or prosecuting offences or contraventions, for processing of data of non-residents under foreign contract, for approved merger, demerger etc. and for locating defaulters and their assets.

### *Setting up and functioning of the Board*

- Comprehensive provisions are now proposed for the setting up and functioning of the Board. These cover the composition of the Board, qualifications and disqualifications of Board Members, their salary, allowances and term of office, and the procedure to be followed for the meetings and inquiry proceedings of the Board.

### *Powers and functions of Data Protection Board*

- Broadly, the Board shall give directions for remediating or mitigating data breaches, inquire into data breaches and complaints and impose financial penalties, refer complaints for Alternate Dispute Resolution and accept Voluntary Undertakings from Data Fiduciaries, and advise the Government to block the website, app etc. of a Data Fiduciary found to repeatedly breach the provisions of the Bill.
- Appeal is now proposed to lie with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

5. During evidence, the representatives of the Ministry stated as follows-

“सर, प्रयास यह रहा है कि बिल संक्षिप्त हो और सरल भाषा में हो, आम आदमी की रोजमर्रा की भाषा में हो। उसके चलते जो हमारा पहले 30 सैक्शन का था, अब करीब 44 सैक्शन उसमें हो गए हैं, लाँ ने भी ड्रॉफिटिंग के कुछ-कुछ चेंजेज किए हैं, सब्सटेंस में उतना चेंज नहीं है, कुछ-कुछ सैक्शंस के मल्टीपल सैक्शंस बने हैं, पर पिछले बिल की तुलना में यह आकार में लगभग आधा है, लेकिन उद्देश्य फिर भी हमारी समझ से पूरा होता है, जो प्रिंसिपल्स बताये गए हैं। हमने इसको सरल तरह से लिखने का प्रयास किया है। हमने उदाहरण दिए हैं, चित्रण दिए हैं, जो जटिल भाषा है, जिसे आम आदमी न समझ पाए, जैसे प्रोविजोज, किन्तु, परन्तु, कि आदि इस टाइप की जो भाषा है, उसे हमने पहली बार इसमें अवाँयड करने की कोशिश की है। इस पूरे कानून में कहीं कोई प्रोविजोज नहीं है और जहाँ तक संभव है, उसे क्रॉस-रिफरेन्सिंग, जिससे उद्देश्य यह है कि जिस आदमी को अपने अधिकार पाने हैं, इस कानून को पढ़कर और जिस बिजनेसेज को इसका पालन करना है, दोनों को स्वयं जहाँ तक हो सके खुद ही कानून को समझ सकें और खुद ही उसका पालन कर सकें और खुद ही अपना हक माँग सकें, इस दृष्टि से कानून को लिखने की हमारी कोशिश रही है।

हमने इस कानून में पहली बार किसी केन्द्रीय लेजिस्लेटिव प्रस्ताव में, परम्परा यह रही है, हम कहते हैं कि पुरुष में महिला भी शामिल है, हमने एक बार महिलाओं के अस्तित्व को स्वीकारते हुए इसमें उल्टा परिभाषित किया है कि 'सी' (She) शब्द का जहाँ उपयोग हुआ है, उसमें 'ही' (He) भी शामिल है।“

## II. The Cyber Conundrum- Addressing the surge of cyber crimes and urgent call for regulatory action

6. The Ministry in its replies commented on the digital India programme as under-

“Digital India Programme is leading the transformation in India for ease of living and digital economy. Digital India proved its resilience during the pandemic and has laid the foundation for adoption of digital initiatives has accelerated in an unprecedented manner. In the post-pandemic world, the progress continues and the same is evidenced by over 40 crore average e-Transactions happening on daily basis and 7.8 billion monthly transactions over UPI worth Rs. 12.8 trillion on December 31, 2022. India’s digital adoption is at rapid pace. With expanded internet access to around 76 crore citizens, the world looks at India as one of the largest Internet user bases with the lowest Internet tariff. India is world leader in Digital Identities; world’s largest Digital Identity Programme with 1.36 billion Aadhaar has helped poor to receive benefits directly in their accounts. This has led to disbursement of Rs. 27.76 lakh crore and led to savings of Rs. 2.2 lakh crore cumulatively till December 31, 2022.”

7. To protect personal data of users, the Central Government, in exercise of its powers under the Information Technology Act, 2000, has prescribed reasonable security practices and procedures and sensitive personal data or information through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These include the requirement that any person collecting, receiving, possessing, storing, dealing or handling information provided should publish on its website a policy for privacy and disclosure of personal information, that such person use the information collected for the purpose for which it was collected and keep it secure, that disclosure of sensitive personal data



be done with prior permission of the information provider, that sensitive personal data or information not be published, and that a third party receiving sensitive personal data or information shall not disclose it further.

8. Section 72A of the Act provides for punishment for disclosure of information in breach of the lawful contract. It provides that any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

9. The Committee asked the Department about the major problems/challenges in ensuring privacy/protection of personal data worldwide in general and in India in particular and how these problems/challenges can be addressed. The Department replied as follows-

“The major problem/challenges associated with the protection of personal data are associated with the entities are as follows:

- i. who determine its purpose and process it for purposes that are unlawful or beyond those for which it was collected, in a non-transparent manner,
- ii. who collect more data than is necessary for the purpose for which it is being collected,
- iii. who store data beyond the period required for meeting such purpose,
- iv. not keeping the data accurate and updated,
- v. unauthorized collection or processing,
- vi. handling data breaches,
- vii. absence of a mechanism to ensure accountability,
- viii. providing rights of the individual with respect to their personal data and
- ix. misleading usage of personal data by individuals.

These problems have been taken care of by applying the following principles while drafting the proposed Digital Personal Data Protection Bill, 2023:

- i. Processing to be done in a fair and transparent lawful manner.
- ii. The personal data be used only for the purpose for which it was collected.
- iii. Only those items of personal data be collected as are required for attaining the specified purpose.
- iv. Personal data not be stored perpetually by default and storage be limited to such duration as is necessary for the specified purpose.
- v. Reasonable effort be made to ensure that the personal data is accurate and kept up to date.
- vi. Reasonable safeguards be taken to prevent personal data breach.

- vii. Entity who decides the purpose and means of processing of personal data should be accountable for such processing with penalty provisions in case of the violation of the provisions of the act.
- viii. Provisioning of rights of obtaining processed personal data, erase/correct the personal data, grievance redressal and nominate another individual for exercising his rights in case of death or incapacity.
- ix. Provisioning of penalty on the individual in case of misleading usage of his data by enforcing duties on them.”

When asked about India's preparedness to deal with recent cyber-attack on India's premier medical institution, the All India Institute of Medical Science (AIIMS), New Delhi and the Ministry plan to deal with vulnerability of healthcare data, the Ministry provided the details as to how proposed Draft Bill is capable of addressing the above issues and prevent such cases in future, given as under:

“The entities collecting the personal data for specified purposes are defined as Data Fiduciaries in the Bill. A large corporate Data Fiduciary, identified as Significant Data Fiduciary, in addition to the general obligations, will have to meet additional obligations like appointing India based data protection officer, conducting data protection impact assessment and data audit.

The Bill entrusts entities to take reasonable security safeguards to prevent personal data breach with respect to the personal data in its possession making them accountable to the individuals. Further, if the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules by the entity is significant, it may, after giving the person an opportunity of being heard, impose monetary penalty.

Also, the Central Government may, on the request of Board that intimates the imposition of monetary penalty on the entity in more than two instances and advises in the interests of the general public, instruct the appropriate agencies/intermediary to block the services of the entity.

In order to sensitize health sector entities regarding latest cyber security threats, a special advisory mentioning best practices to enhance resiliency of health sector entities was prepared by CERT-In and sent to Ministry of Health & Family Welfare in December 2022, requesting to disseminate the advisory to all authorised medical care entities/ service providers in the country.

Following are salient best practices suggested to enhance resilience of health sector:

- i. Formulate cyber security policy and assign roles and responsibilities for Chief Information Security Officer (CISO) and a dedicated cyber security functional team.

- ii. Audit the entire ICT infrastructure and deploy appropriate security controls based on the audit outcome. Services of 150 CERT-In empanelled auditors may be utilized.
- iii. Prepare, test and implement Business Continuity Plan (BCP) and Disaster Recovery (DR) plan
- iv. Upgrade any outdated operating systems & applications and update patches on regular basis
- v. Maintain secure offline backup for critical databases
- vi. Create a structured network with network segmentation. Review and revamp the complete network architecture in security perspective for better visibility, management and control of IT resources.

CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

CERT-In has published “India Ransomware Report H1 – 2022” in August 2022, covering latest tactics and techniques of Ransomware attackers along with sector wise trends observed in the first half of year-2022, specific to Indian cyber space. The report also describes ransomware specific Incident response remediation and mitigation measures. “India Ransomware Report – 2022” has also been published by CERT-In in April 2023 covering methods of ransomware attacks and mitigation measures.

Ministry of Home Affairs has created a National Counter Ransomware Taskforce comprising of multiple stakeholders to formulate strategies to effectively tackle ransomware threats and put in place proactive and responsive systems by stakeholders. The Taskforce comprises working groups on Cooperation & Diplomacy, Incident Response, Security Cluster, Awareness & Capacity Building.”

### **III. Inclusive and Comprehensive Consultation Journey for Comprehensive Solutions**

10. Keeping in view the need to strengthen the law on protection of personal data, the Government had introduced the Personal Data Protection Bill, 2019 in Parliament. In the light of the understanding that emerged as a result of consultations with stakeholders in connection with the drafting of the Bill and its consideration by the Joint Committee of Parliament, the Government withdrew the 2019 Bill. On 18.11.2022, Government published the aforesaid new draft Bill, titled “the Digital Personal Data Protection Bill, 2022”, and invited feedback from public and initiated stakeholder and inter-ministerial consultation on the Bill.

**Regarding the comments received on the draft Bill published for public consultation and inter-Ministerial consultation initiated, the Ministry reply as under:**

“Comments on the draft Bill were invited from the public on 18.11.2022 and the last date for receipt of comments was 2.1.2023. Further, inter-ministerial consultation was also initiated on the Bill. In the period, Ministry has also received feedback from 45 Ministries/ departments, 21,666 comments from public and feedback received from various other stakeholders such as Indian and other international organizations also. Similarly, there have been some evolution in our understanding also of the issues and the ways to address them. In the light of these, the Draft Bill has been relooked into and is ready for approval.”

11. The Committee asked the Ministry, if the new draft Bill combines the features of the present piecemeal legislation and how does the new Bill plan to protect the use of data for other than intended purposes by both State and non-State actors. The Ministry replied that -

“In the absence of well-defined rights and obligations of individuals and entities responsible for data processing, the interests of stakeholders are not adequately safeguarded. While drafting the proposed DPDP Bill, 2023 the rights and consent based model approach has been appropriately balanced. Every entity responsible for processing the personal data of an individual must obtain the consent of such individual, except in few instances where the personal data processing can be done for certain legitimate uses, while simultaneously providing appropriate rights to the individual making data processing entities accountable to the individual also. The rights enshrined in the draft Bill are to obtain the summary of the data processed, to correct or erase the personal data, to grievance redressal and to nominate in case of death or incapacity of the individual.

The Bill aims to establish a comprehensive legal framework governing digital personal data protection, by framing out the rights and duties of Data Principals and the obligations of Data Fiduciaries, empowering Data Principals and fixing the accountability of Data Fiduciaries. One of the core principles while drafting the Bill was the purpose limitation i.e., use of personal data only for the purpose specified at the time of obtaining consent of the Data Principal.

The provisions of the Bill cast specific obligations on Data Fiduciaries, both State and non-State, in data processing; make reasonable efforts to ensure accuracy and completeness of data; implement technical and organisational measures; take reasonable security safeguards to prevent personal data breach; and engage/use a Data Processor only under a valid contract among others. If they fail to fulfil their obligations, they shall be liable to pay financial penalty as provided for under the proposed legislation, after due opportunity of being heard by the Data Protection Board.”

#### IV. Globally Aligned Bill- Embracing International Best Practices

12. On the issue of on Global legal frameworks for Data Privacy and Security, the Ministry spelled out principles involved along with its features-

“While formulating the Bill, the Government considered global best practices while reviewing the personal data protection laws of Singapore, Australia, European Union and the prospective federal legislation of the United States of America. The following principles have formed the key principles underlying the personal data protection laws in various other jurisdictions and are also the principles underlying the Bill:

- The principle that usage of personal data by organisations must be done in a lawful manner, which is fair and transparent to the Data Principals.
- The principle of purpose, i.e., the personal data be used only for the purpose for which it was collected.
- The principle of data minimisation, i.e., only those items of personal data be collected as are required for attaining a specific purpose.
- The principle of accuracy of personal data, i.e., reasonable effort be made to ensure that the personal data is accurate and kept up to date.
- The principle of storage limitation, i.e., personal data not be stored perpetually by default and storage be limited to such duration as is necessary for the stated purpose for which it was collected.
- The principle that reasonable safeguards be taken to ensure that there is no unauthorised collection or processing of personal data, so that personal data breach may be prevented.
- The principle that the person who decides the purpose and means of processing of personal data should be accountable for such processing.

Further, like the data protection laws in the other mentioned jurisdictions, the Bill too has the following features:

- (i) It is technology-agnostic.
- (ii) It provides for financial penalties (rather than criminalisation).
- (iii) It specifies the obligations of Data Fiduciaries based on the aforesaid seven principles.
- (iv) It provides for additional obligations for certain Data Fiduciaries (referred to as Significant Data Fiduciaries in the Bill), similar to the approach followed in the data protection laws of the European Union and Singapore.
- (v) It provides for additional obligations/safeguards for processing of personal data of children, which is similar to the approach followed in the data protection law of Singapore.

(vi) It provides for the rights of Data Principals, which is similar to the provisions in the data protection laws of the European Union, Australia and Singapore.

(vii) It provides for cross-border data transfer. The European Union and Singapore also have provisions for such transfer.

The legal framework for data privacy and security in India has evolved over the years, and it continues to develop in response to the rapid growth of digital technology and data-driven activities.”

13. The proposed Bill seeks to minimise disruption by making provision for the following:

- a. Allowing for continuing validity of processing based on pre-existing consent (unless withdrawn), while requiring Data Fiduciary to notify the Data Principal;
- b. Making provision for consistency with sectoral laws, so that the basic protection is ensured under the Bill while additional regulation/protection may continue to be applicable under sector-specific law; and
- c. Enabling processing outside India, while retaining India’s right to restrict processing in notified countries.

14. The proposed Bill, while retaining the core principles of data protection in the earlier Bill (notice for collecting or processing personal data, consent, purpose and storage limitation, accuracy of data, etc.), offers a simpler law which is easy to understand and administer. Examples of this include the following:

- a. There is no classification of personal data, which is sought to be protected as a whole, thereby avoiding issues of interpretation and classification-based protection.
- b. In addition to the rights under the earlier Bill, the proposed Bill also includes the right to nominate a person to exercise rights in the event of death or incapacity of the Data Principal. Further, associated are duties entrusted to an individual.
- c. It defines the obligations of Data Fiduciaries and fixes accountability for breach in their observance without adding to compliance burden.

## **V. Unleashing the Digital India Bill**

15. The Committee put forth a query about the weaknesses identified in the IT Act that restrict stringent implementation of Penal provisions under the IT Act and the provisions of IT Act that are likely to be struck down with the enactment of DPDP Bill. The Committee further enquired about how is the proposed Digital India Bill likely to

strengthen the implementation mechanism and aid/ supplement DPDP Bill in its effective implementation. The Ministry gave the following reply-

“As of today, to protect personal data of users, the Central Government, in exercise of its powers under the Information Technology Act, 2000, has prescribed reasonable security practices and procedures for sensitive personal data or information through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These include the requirement that any person collecting, receiving, possessing, storing, dealing or handling information provided should publish on its website a policy for privacy and disclosure of personal information, that such person use the information collected for the purpose for which it was collected and keep it secure, that disclosure of sensitive personal data be done with prior permission of the information provider, that sensitive personal data or information not be published, and that a third party receiving sensitive personal data or information not disclose it further.

While these rules obligate persons collecting and processing data to ensure reasonable security practices and procedures, there is need to have a more detailed framework that provides for rights and duties of individuals to whom digital personal data relates and the obligations of persons who determine the purpose and means of processing of such personal data. Keeping in view the need to strengthen the law on protection of personal data and bringing a comprehensive framework, the current proposal of Digital Personal Data Protection Bill is submitted.

The Information Technology Act, 2000 shall be amended in the following manner, namely:—

(a) section 43A shall be omitted[Section 43A inter-alia provides for compensation for failure to protect data.--Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.]

(b) in section 81, in the proviso, after the words and figures “the Patents Act, 1970”, the words and figures “or the Digital Personal Data Protection Act, 2023” shall be inserted; and

(c) in section 87, in sub-section (2), clause (ob) shall be omitted.”

## VI. Need for amendments in IT Act

16. During evidence, the Committee raised the issue of amendment in the IT Act as follows-

*“In the last few years, we see very less or even almost nil convictions with respect to reported cyber crimes or cyber offences. In fact, the Committee had asked details from the MHA on the number of convictions versus number of FIRS that have taken place. But I do not think the details have been given to the Committee. It will prove that how ineffective the IT currently is and that is the reason why a concerted effort has to be made to revisit the struck down provision of the IT Act because it not only deals with the issues that ..... highlighted but also the problem of the exemption of liability of social media intermediaries. Even that is a grey area. That also needs to be addressed and therefore, there should be revisiting of the struck provisions of the IT Act in such a manner that it is congruent with the constitutional spirit. It needs to be done. Otherwise, the expectation that the criminalisation or criminality that exists in the IT Act will compliment the provisions here may not be effective and will not suffice. “*

17. Further, during evidence, the representatives of the Ministry submitted that –

**“ मैं उन पर अभी बताना चाहूंगा। मैं 66ए वाले इश्यू से ही स्टार्ट करता हूँ। सुप्रीम कोर्ट ने 66ए स्ट्रक डाउन किया है, लेकिन 66 के बाकी प्रोविजन्स अभी भी हैं। उससे ज्यादा अच्छा काम यह है और सर आप सही कह रहे हैं कि आई टी एक्ट वर्ष 2000 में बना था, लेकिन अभी डिजिटल इण्डिया एक्ट को बहुत ही जल्दी आपके मार्गदर्शन के साथ आपके समक्ष लाने की कोशिश कर रहे हैं। उसका ड्राफ्ट लेवल पर काम चल रहा है।“**

## VII. Ensuring Robust Safeguards Within the Bill For Inclusive Digital Access

18. Broadly, the safeguards proposed for processing of personal data of children include processing only with parental consent and not undertaking processing



detrimental to children’s well-being or involving tracking, behavioural monitoring or targeted advertising. However, to enable use in cases like protection of abandoned children, etc., Government may notify purposes where processing may be allowed without parental consent or with tracking etc.

19. Regarding the provisions to protect the data of digitally illiterate person, the Ministry submitted as follows-

“The bill recognizes the need for the consent framework to adapt and improve over time for the processing of the personal data. The Bill includes provisions that enable the establishment of prescribed methods for obtaining consent and delivering notices. As the bill progresses, the consent and notice mechanisms may even incorporate visual elements, allowing for easier understanding and accessibility. By incorporating these enabling provisions, the bill aims to extend its benefits to digitally illiterate individuals, ensuring their inclusion in the evolving landscape of data privacy and protection.”

### **VIII. Enhancing Citizen Awareness and Safeguarding Digital Personal Data**

20. The Ministry, while explaining various features of the Bill, put forth the facts as under-

“The Draft DPDP Bill, 2023 enhances the ease of doing business as well as ease of living. It has enabled faster resolution of disputes by Board by referring matters for the Alternate Dispute Resolution through a mediator identified by the parties and by accepting Voluntary Undertakings from Data Fiduciaries to enable faster resolution.

As far as compensation is concerned, any individual who suffers a civil wrong can invoke legal liability as a claimant against the person committing such wrongful act for compensatory damages, under torts law. A person who suffers a civil wrong on account of violation of her rights or non-compliance of obligations by a Data Fiduciary may raise such a claim before a civil court in consequence of such wrong. Such a person could also cite any penalty imposed by the Board for non-compliance as material in support of his/her claim. The draft Bill has adequate provisions enabling an individual for exercising his rights over his personal data. The provisions of the Bill are not applicable on notified State entities only in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to these.

These grounds are reflected in article 19(2) of the Constitution, which provides for making of law that imposes reasonable restrictions on exercise of the right guaranteed by article 19. Also, exemption has been provided to Government regarding retention of personal data, so that the Government may continue to have information regarding various actions taken in respect

of individuals, which may be required for various legitimate purposes such as law enforcement, looking into complaints and grievances, follow-up of audit observations and delivery of benefits.

The Bill does not provide for surveillance of Data Principal in any form. It is to be noted that lawful interception and monitoring is done by the authorised law enforcement agencies after due authorisation by the Central Government or the State Government concerned. It is governed by the provisions contained in sub-section (2) of section 5 of the Indian Telegraph Act, 1885 read with Rule 419A of Indian Telegraph Rules, 1951 and section 69 of the Information Technology Act, 2000 read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.”

21. Regarding the role of PM Disha Scheme in spreading digital literacy among masses, the Ministry provided the following information-

“The Government of India has approved a scheme titled “Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA)” to usher in digital literacy in rural India by covering 6 crore rural households (one person per household). To ensure equitable geographical reach, each of the 2,50,000 Gram Panchayats across the country are registering an average of 200-300 candidates. Special focus of the said Scheme is on training the beneficiaries on use of Electronic Payment System. The outcome measurement criteria include undertaking at least 5 electronic payments transactions by each beneficiary using UPI (including BHIM app), USSD, PoS, AEPS, Cards, Internet Banking. As on 31st October, 2022, a total of 6.51 crore beneficiaries have been enrolled, out of which training has been imparted to 5.59 crore beneficiaries, out of this more than 4.15 crore beneficiaries have been certified under the PMGDISHA Scheme.”

## **IX. Significance of Consent in the Draft Bill**

22. Before requesting consent, the Data Fiduciary must give a notice specifying the purpose for which data will be processed, with the option to access it in any of the Indian languages listed in the 8<sup>th</sup> Schedule to the Constitution. Consent given shall be limited to personal data necessary for such purpose, and the giving of consent for personal data not necessary for the purpose may not be made a condition for processing. It shall be withdrawable at any time.

23. Consent Managers accountable to the Data Principal may serve as single points of contact to enable them to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform.

24. To avoid disruption, where the Data Principal has given consent before the proposed enactment, the Data Fiduciary shall be obligated to give notice regarding the same to the Data Principal, while continuing to process the data, unless consent is withdrawn.

25. The Committee wanted to know whether the proposed Bill provides for “anytime withdrawal of consent” or “Lapsable Consent” to be specifically mentioned in the notice while the consent is being obtained from the data principal. The Department responded as follows-

“As per the provisions of the bill, Data Principal has the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given. The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.”

26. During evidence, the representatives of the Ministry stated as follows-

*“On consent, first of all, as we put out in the draft Bill, we had said that it must be in clear and simple language. The draft as it currently stands, it will be prescribed through rules. So, we had already said, it would be clear and plain. It would have the option on the click to view and access in Indian language, your own language. In addition, as I mentioned in the presentation, in our discussions our intent is also that when we put in the rules, we are going to ask them to make it visible through videos and animations so that it not legally, it is actually understandable which is precisely the point you are making. So, we certainly intend to do that. The second point which you said that it becomes mandatory that you cannot proceed. We are doing what no other country has done. In our draft, now we are saying that if you take consent which is beyond what is necessary for the stated, specified purpose, it is illegal. Just like an illegal contract is no contract, this will be an illegal consent. So, even if I consent and I access, I will continue to be liable because it is a question of fact whether to do this. Suppose I say that I am going to underwrite your loan and I take so much information. Now, I also say that I want your mobile contact list. If I give a mobile contact list and I have taken consent for that, tomorrow if it is called into question how did you take a consent for contact list of my mobile phone for underwriting a loan, it cannot be justified. So, if he has taken, he would be liable for committing a breach. So, if he takes data beyond what is necessary, it is illegal by law. The law deems it to be illegal. Today, it is unregulated. “*

27. Further, during evidence, the representatives of the Ministry stated as follows-  
“जब हम नोटिस वाला नियम बनाएंगे तो उसमें लिख देंगे कि आप विदड़ा कर सकते हैं, उसी स्टेज पर लेते समय बताया जाएगा कि आप जब चाहें विदड़ा कर सकते हैं, यह इमीडिएट भी हो सकता है और एक महीने बाद की स्पेसिफाइड डेट से भी कर सकते हैं।”

#### **X. Certain exemptions (Legitimate Uses) to Maintain Public Order**

28. The provisions regarding exemptions have also been revisited in light of the feedback and, broadly, the exemptions now proposed include processing by the State and its notified instrumentalities in the interests of sovereignty, integrity, security of the State, friendly foreign relations, public order or incitement of related offence. They also include processing for research, archiving or statistical purposes, for startups or other notified categories of Data Fiduciaries, for enforcement of legal rights and claims, for performance of judicial or regulatory functions, for preventing, detecting, investigating or prosecuting offences or contraventions, for processing of data of non-residents under foreign contract, for approved merger, demerger etc. and for locating defaulters and their assets.

29. Taking into account the feedback received, processing of personal data for certain legitimate uses is now proposed to be more focussed than in the draft published for public consultation. Broadly, such uses would include performance by the State and its instrumentalities of functions under law, or in the interest of sovereignty, integrity and security of the State, or for providing/issuing subsidies, benefits, services, certificates, licences and permits prescribed by rules. They would also include disclosures for fulfilling any obligation under law, compliance with any judgement or order under law, protection/assistance/service in a health emergency, disaster or public order situation, and in relation to employees.

30. With regard to the reasonable purposes for which data can be processed with deemed consent, the Department informed the following-

“In the earlier DPDP Bill, 2022 draft the deemed Consent was applicable only when a data principal was deemed to have given consent for her personal data if such processing is necessary for the specific conditions only including public order, employment etc.. The deemed consent clause has been henceforth removed after the consultation and feedback received from stakeholders. In the modified draft of DPDP Bill, 2023, in its equivalent format, the personal data can be processed for certain legitimate uses. These are as under:

- (i) For the State and its instrumentalities to perform functions under law or in the interest of sovereignty and integrity of India and security of the State
- (ii) For the State and its instrumentalities to provide or issue subsidies, benefits, services, certificates, licences and permits that are prescribed through rules
- (iii) To comply with any judgement or order under law
- (iv) To protect or assist or provide service in a medical or health emergency, disaster situation or maintain public order and
- (v) In relation to an employee.”

31. Further, during evidence, the representatives of the Ministry stated that-

*“सर, एग्जम्पशंस की जहां तक बात है तो सिक्योरिटी, सॉवेरेन्टी, पब्लिक ऑर्डर इत्यादि के लिए हमारी सिक्योरिटी की जो नोटिफाइड एजेंसीज हैं, उनके कामकाज के लिए, रिसर्च, स्टैटिस्टिकल आर्काइविंग के लिए, स्टार्ट-अप्स के लिए, और लीगल, ज्युडिशियरी, रेगुलेटरी, लॉ एन्फोर्समेंट इत्यादि के लिए डेटा एग्जम्पशंस का प्रावधान है। डेटा प्रोटेक्शन बोर्ड में उन्हें इसका पूरा अधिकार होगा कि वे डेटा ब्रीचेज की जांच करें, शिकायत की जांच करें, पेनाल्टीज लगाएं, उसकी रोकथाम के लिए दिशा-निर्देश दें, मीडिएशन इत्यादि के जरिए उसका निपटारा करें। अगर कोई बार-बार उल्लंघन करता है तो वे सरकार को उसके बारे में रिकमेंड कर सकते हैं और सरकार यह आदेश कर सकती है कि जनहित*

*में इसकी वेबसाइट इत्यादि को ब्लॉक कर दिया जाए, जिससे लोगों को भविष्य में कोई और नुकसान न हो।“*

**XI. Accountability and Deterrence Mechanism under the Digital Personal Data Protection Bill**

32. The Committee enquired about the provisions that have been made to provide compensation to data principal in case of data breach. The reply of the Ministry is as follows-

“Determination of compensation of any significant amount is ordinarily a judicial function performed by civil courts or tribunals specially empowered in this behalf. The Data Protection Board is not a court or a tribunal. Any individual who suffers a civil wrong can invoke legal liability as a claimant against the person committing such wrongful act for compensatory damages, under torts law. A person who suffers a civil wrong on account of violation of her rights or non-compliance of obligations by a Data Fiduciary may raise such a claim before a civil court in consequence of such wrong. Such a person could also cite any penalty imposed by the Board for non-compliance as material in support of his/her claim.”

33. Further, to a query on deterrent clauses against the big tech companies who commit an offence of data breach, the Ministry responded that-

“The companies collecting the personal data for specified purposes are defined as Data Fiduciaries in the Bill. A large corporate Data Fiduciary can be identified as Significant Data Fiduciary (SDF) on the basis of the specific criteria. These SDF, in addition to the general obligations, will have to meet additional obligations like appointing India based data protection officer, conducting data protection impact assessment and data audit. In addition to these obligations, to make Data Fiduciaries accountable for the data processing, there are provision to impose financial penalty by data protection board in case of personal data breach by data fiduciaries after due inquiry under the principle of natural justice. . The Bill entrusts entities to take reasonable security safeguards to prevent personal data breach with respect to the personal data in its possession making them accountable to the individuals. Further, if the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules by the entity is significant, it may, after giving the person an opportunity of being heard, impose monetary penalty. Also, the Central Government may, on the request of Board that intimates the imposition of monetary penalty on the entity in more than

two instances and advises in the interests of the general public, instruct the appropriate agencies/intermediary to block the services of the entity.”

34. Further, during evidence, the representatives of the Ministry stated that-  
“महोदय, इसके अलावा ऑब्लिगेशंस हैं। इनके कुछ जनरल ऑब्लिगेशंस रहेंगे, डेटा लेने वाले और प्रोसेस करने वाले के होंगे। वह कानूनन हो, फेयर ट्रांसपैरेंसी हो, जिसका मैंने पहले जिक्र किया है। ये डेटा फिड्यूशियरी के अंतर्गत हैं। कुछ विशिष्ट मामले हैं, जैसे बच्चों के मामले में उनको ज्यादा प्रोटेक्शन की जरूरत है, जो सिग्निफिकेंट डेटा फिड्यूशियरी है, जो बड़े पैमाने पर डेटा से डील करते हैं, उनके ऑब्लिगेशन के स्तर हायर होने चाहिए। उनकी जिम्मेदारियां कुछ अधिक होनी चाहिए, तो कुछ एडिशनल ऑब्लिगेशंस होने चाहिए। ऐसा कुछ देशों में है। न केवल जिम्मेदारियां अधिक हों, बल्कि उसके लिए कुछ सेफगार्ड्स भी हों। जैसे कि एक डेटाप्रोटेक्शन ऑफिसर हो, वह इस चीज के लिए जिम्मेदार हो। वह सीधे कंपनी के बोर्ड को रिपोर्ट करे। वह इंडिपेन्डेंट डेटाऑडिटर्स से इंडिपेन्डेंट ऑडिट कराए और डेटा प्रोटेक्शन इम्पैक्ट असिसमेंट करे। वह खुद ही नियमित तौर पर जांच करे। ऐसे कुछ-कुछ अतिरिक्त दायित्व उनको दिए जाते हैं। फेडरल एप्लीकेशन में पर्सनल डेटा ऑफ चिल्ड्रेन का है, जिसमें पैरेंट का कंसेन्ट होना चाहिए। एज का वैरिफिकेशन होना चाहिए, वरना कैसे पता चलेगा कि किस उम्र का है। हमारे यहां पर 18 साल के हिसाब से है। ट्रेकिंग बिहेवियरल मॉनीटरिंग, टारगेटिंग एडवरटाइजिंग वगैरह के मामले में इसमें रोक है। ये तो ऑब्लिगेशंस और दायित्व हैं और ऐसे ही अधिकार हैं। राइट्स ऑफ डेटा प्रिंसिपल्स हैं और क्रॉस बॉर्डर डेटा प्रोटेक्शन है।”

35. With regard to the mechanism that has been devised in the proposed DPDP Bill to fast track prosecutions, the Ministry stated that -

“The proposed DPDP Bill does not provision any criminal liability, the liabilities envisaged are civil in nature. However, provisions of existing laws will continue.”

36. During evidence, the representatives of the Ministry further stated that –

“महोदय, हमारी कोशिश है कि दंड वगैरह और सुनवाई से प्रक्रिया लम्बी हो जाती है। हमें लोगों को रिलीफ देने पर ज्यादा फोकस करना है

इसलिए मिडिएशन के जरिए ग्रीवांस सॉल्व करने पर जोर दिया है। यदि वह स्वयं ही गलती स्वीकार करते हुए बोर्ड के सामने प्रस्ताव रखे कि मैं अंडरटेकिंग देता हूँ तो बोर्ड उसे स्वीकार करते हुए मामले को रोक सकता है। यदि बाद में उसका उल्लंघन होता है, तो उसे सीधे-सीधे दंड मिलेगा लेकिन दंड देने की जगह उसे रिलीफ देने की दिशा में बढ़ा जाए जिससे कि समस्या का निदान जल्द हो सके। एकाउंटेबिलिटी के लिए मोनिटरी पैनल्टी पर, फाइनेंशियल पैनल्टी पर बल दिया है। क्रिमिनल ऑफेंसेज आज भी हैं। जैसे क्रिमिनल ब्रीच ऑफ ट्रस्ट होता है, यदि जानते हुए एक का डेटा दूसरे को देता है तो आईपीसी में धारा 405 में ब्रीच ऑफ ट्रस्ट है। हमारे आईटी एक्ट में यदि गलत तरीके से डेटा को लिया या दिया जाता है, तो धारा 43 का वॉयलेशन है और धारा 46 के तहत कारावास का दंड भी दिया जा सकता है।”

37. Broadly, the proposed obligations of the Data Fiduciary will include implementation of technical and organisational measures for compliance, security safeguards to prevent data breach, intimation of data breaches to affected Data Principals and the Data Protection Board, erasure of data upon withdrawal of consent or when retention is no longer necessary for the specified purpose, publishing of contact details of person to answer queries of Data Principals, establishing of a grievance redressal system, and use of Data Processors only under contract.

38. Further, certain additional obligations are proposed in respect of Data Fiduciaries notified as Significant Data Fiduciaries, such as appointing a data auditor and conducting periodic Data Protection Impact Assessment to ensure higher degree of data protection.

39. To a query about the obligations of Data Fiduciaries, the Ministry replied as follows-

“The companies collecting the personal data for specified purposes are defined as Data Fiduciaries in the Bill. A large corporate Data Fiduciary can be identified as Significant Data Fiduciary (SDF) on the basis of the specific criteria. These SDF, in addition to the general obligations, will have to meet additional obligations like appointing India based data protection officer, conducting data protection impact assessment and data audit. In addition to



these obligations, to make Data Fiduciaries accountable for the data processing, there are provision to impose financial penalty by data protection board in case of personal data breach by data fiduciaries after due inquiry under the principle of natural justice. . The Bill entrusts entities to take reasonable security safeguards to prevent personal data breach with respect to the personal data in its possession making them accountable to the individuals. Further, if the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules by the entity is significant, it may, after giving the person an opportunity of being heard, impose monetary penalty. Also, the Central Government may, on the request of Board that intimates the imposition of monetary penalty on the entity in more than two instances and advises in the interests of the general public, instruct the appropriate agencies/intermediary to block the services of the entity.”

## **XII. Flexibility and evolvability of the provisions of the draft Bill**

40. On the issue of laws governing data privacy and the implications for the AI community, the Ministry submitted as follows-

“The DPDP Bill, 2023 empowers the Central Government to exempt, the application of the provisions of the proposed legislation to the processing of personal data necessary for research purposes, if the personal data is not to be used to take any decision specific to a Data Principal and processing is carried on in accordance with specified standards. This provision may be made use of to address any concerns regarding data availability for AI research. Further, the Bill is not applicable to data made publicly available by Data Principals or pursuant to any obligation by law to disclose such data, making available sizeable volumes of data for AI research. Information Technology is undergoing evolution at a very fast pace with huge social and economic impact, thus law governing it should have sufficient flexibility to address changing situations and emerging requirements. Therefore, while the Bill sets out the rights and duties of Data Principals and the obligations of Data Fiduciaries, it attempts to retain sufficient flexibility to address such requirements. The DPDP, 2023 has been drafted as a technology agnostic legislation as the digital technology is undergoing evolution at a very fast pace with huge social and economic impact, thus law governing it should have sufficient flexibility to address changing situations and emerging requirements. Therefore, while the Bill sets out the rights and duties of Data Principals and the obligations of Data Fiduciaries, it attempts to retain sufficient flexibility to address such requirements.”

41. Many provisions in the Bill have a clause saying “as may be prescribed” or its equivalence. The Ministry explained it as follows-

“The Draft DPDP Bill, 2023 comprises appropriate rulemaking provisions. Information Technology is undergoing evolution at a very fast pace with huge social and economic impact, thus law governing it should have sufficient flexibility to address changing situations and emerging requirements. Therefore, while the Bill sets out the rights and duties of Data Principals and the obligations of Data Fiduciaries, it attempts to retain sufficient flexibility to address such requirements. Further, most of the matters that are ‘prescribed by rules’ are matters of procedure and detail, which it may not be practicable to provide for in the Bill itself. Moreover, every rule made has to be laid in the Parliament for its acceptance, modification or annulment.”

42. The Committee raised concerns raised during one of its Sittings on various matters including ‘rule making’ powers of Central Government. The Ministry responded to the concerns as follows-

“The current draft of DPDP Bill, 2022 has been prepared considering the dynamic nature of the subject as the threat landscape keeps evolving at a high pace where dynamic decision making and changes in the processes are desired to counter the ever evolving the threat landscape. Owing to the explained dynamicity, to address the public concerns as the challenges evolve and to provide sufficient adaptability, the draft Bill provides for rule-making power to the Central government. The Rules are to be laid in the Parliament. The delegations are more of routine in nature and are provided in every legislation to make implementation practical and feasible.”

## PART-II

### RECOMMENDATIONS

#### “Citizen Data Security & Privacy”

##### Introductory- Need For Dedicated Legislation on Data Privacy:

1. In recent years, personal data protection issues have gained significant attention in public discussions and debates. It has become evident that while the Internet and technology bring about positive connectivity, they also create an environment where user harm and misuse can thrive in the absence of appropriate rules and laws. To address these concerns, it is crucial for laws and regulations governing the Internet to be built upon foundational principles of openness, safety, trust, and accountability.

The Supreme Court, in the matter of Justice K. S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors., has recognized the right to privacy as an essential part of the fundamental rights guaranteed by the Constitution. The Court commended the Union Government to put into place a robust regime for data protection. This landmark judgment highlights the significance of protecting privacy in the digital age.

In light of the growing significance of protection of citizen’s personal data and the need to strengthen data protection laws, the Government introduced the Personal Data Protection Bill, 2019, in the Parliament in December, 2019. After consideration, the Bill was referred to the Joint Committee of Parliament, which engaged in consultations and submitted a Report. Taking into account feedback from stakeholders and various agencies, the Bill was, however, withdrawn in August, 2022.

Subsequently, on November 18, 2022, the Government published a new draft Bill, titled the Digital Personal Data Protection Bill, 2022, and initiated public consultation on this. The Observations/Recommendations of the Committee are given under the subsequent paragraphs.

## **The Cyber Conundrum- Addressing the Surge of Cyber Crimes And Urgent Call For Regulatory Action:**

2. The Committee acknowledge that data in general and personal data in particular are at the core of this fast-growing digital economy and ecosystem of digital products, services and intermediation. In the post-pandemic world, this progress has been exemplified by the staggering number of e-transactions, with over 40 crore transactions occurring daily, and the immense volume of UPI transactions, totaling Rs. 12.8 trillion, on December, 2022. India's digital adoption has been remarkable, providing internet access to approximately 76 crore citizens.

However, amidst this global digital transformation, the Committee recognize the dual nature of the digitization of personal data. While it has revolutionized service delivery and significantly improved the ease of living, it has also exposed individuals to mounting vulnerability due to the growing risk of personal data misuse. To address this concern, the Governments around the world have responded by enacting data protection laws to safeguard digitized personal data. The Committee are also conscious of the fact that in addition to the global impact, recent cyber-attacks on India's prestigious medical institution, have exposed the deficiencies to counter such attacks, in the absence of a comprehensive data protection law. The Committee firmly believe that in the absence of well-defined rights and obligations of individuals and entities responsible for data processing, the interests of stakeholders are not adequately safeguarded. The Committee are of the firm opinion that there is an urgent need to introduce a data protection law, that effectively combats the growing menace of cybercrime, ensures public order and also strengthens India's defense capabilities. Hence, the Committee emphasize the imperative need for enactment of an appropriate law to ensure comprehensive and robust safeguards for citizens' data security and privacy in an ever-evolving digital landscape.

**Inclusive and Comprehensive Consultation Journey for Comprehensive Solutions:**

3. The Committee have been informed that Ministry has undergone a thorough and comprehensive process of consultation thereby ensuring comprehensive input from various stakeholders while drafting the Bill to safeguard citizen's data and privacy. The Committee observe that the Ministry had invited public comments on the draft Bill in 2022. Further, inter-ministerial consultations were initiated to gather feedback ~~on the Bill~~. The Committee were informed that along with the people's feedback, the Ministry also received feedback from 45 Ministries/Departments, a total of 21666 comments were received from various stakeholders. Subsequently, the Parliamentary Standing Committee were briefed on the intricacies of the subject 'citizen's data security and privacy' in December, 2022 and June, 2023. The Committee are pleased to learn that the concerns raised during these meetings, regarding the "rule-making" powers of the Central Government, compensation from data fiduciaries, duties on data principals, and the establishment of a grievance redressal system for data principals, etc., have been suitably incorporated in the Draft Bill. The Committee exhort and recommend that the Ministry will not be complacent and will actively pursue necessary improvements to the legislation to effectively adapt to the ever-evolving and dynamic nature of digital technologies whenever the need arises.

4. The Committee have been informed that the Ministry is in a process of enacting a law with a purpose to establish a robust framework for the processing of digital personal data by striking a balance between safeguarding individuals' rights to protect their personal data and facilitating lawful data processing activities. This draft legislative initiative draws inspiration from internationally recognized principles that underpin personal data protection laws in diverse jurisdictions. For instance; the principle that usage of personal data by organisations must be done in a lawful manner, which is fair and transparent to the Data Principals; the principle of purpose, i.e., the personal data be used only for the purpose for which it was collected; the principle of data minimisation, i.e., only those items of personal data be collected as are

required for attaining the specified purpose; the principle of accuracy of personal data, i.e., reasonable effort be made to ensure that the personal data is accurate and kept up to date; the principle of storage limitation, i.e., personal data not be stored perpetually by default and storage be limited to such duration as is necessary for the specified purpose; the principle that reasonable safeguards be taken to prevent personal data breach; the principle that the person who decides the purpose and means of processing of personal data should be accountable for such processing.

The Committee firmly believe that the implementation of the a suitable legislation to safeguard citizen's data and privacy will be a much needed step in the domain of data processing, as it effectively brings the previously unregulated landscape under comprehensive regulation in a seamless and non-disruptive manner. In this regard, the Committee are of the considered view that enactment of such a law will herald a new era of enhanced data security and privacy protection, ensuring the safeguarding of personal information and fostering trust in the digital ecosystem.

5. Regarding the proposed Digital Personal Data Protection Bill, published by the Ministry in November, 2022 the Committee has been apprised that its primary objective is to establish a comprehensive legal framework that governs the protection of digital personal data. The Bill addresses the previously unregulated realm of data processing in a manner that minimizes disruption for all stakeholders, including Data Principals, Data Fiduciaries, regulatory bodies, and both State and non-State entities. It ensures consistency with existing laws and serves as a horizontal legislation that applies to various entities, encompassing the State and its instrumentalities, and non-State actors alike. The Committee observe that the proposed Digital Personal Data Protection Bill incorporates a number of innovative features, viz., for the first time in any Central Act or Bill, women have been acknowledged by using the feminine pronoun "she" for a person. It also provides Data Principals the option of giving consent for personal data processing in any language enumerated in the Eighth Schedule to the Constitution. The Committee were apprised that while drafting,

it has been ensured that the rights and consent based model approach is appropriately balanced.

The Ministry informed that it offers a simpler law which is easy to understand and administer. The Committee appreciate that unlike the previous Bill i.e. Personal Data Protection Bill, 2019, the proposed Bill consciously follows an approach of providing for protection of personal data as a whole, without further classification, thereby avoiding issues of interpretation and classification-based protection. The Data Bill aims to strike the right balance between rights, commerce and innovation.

In view of the above, the Committee have every reason to believe that enactment of a comprehensive law on citizen's data security and privacy will have various tangible benefits such as enhancing data security measures, fortifying privacy protections, fostering greater transparency and accountability in data processing practices, empowering individuals with greater control over their personal information, and instilling public confidence in the digital ecosystem.

**Globally aligned - embracing international best practices:**

6. The Committee have been apprised that the Government has made all out effort in formulating the Bill by taking into account best global practices observed in the personal data protection laws of Singapore, Australia, the European Union, and the prospective federal legislation of the United States of America. The Committee have been informed that the fundamental principles that underpin personal data protection laws in various jurisdictions, also form the basis of the Draft Digital Personal Data Protection Bill. These principles include the lawful, fair, and transparent usage of personal data by organizations, the principles of purpose, data minimization, accuracy, storage limitation, and the need for reasonable safeguards. It is encouraging to find the Ministry's submission that the Bill aligns with the data protection laws of other jurisdictions, featuring financial penalties instead of criminalization, imposing additional obligations on specific Data Fiduciaries (known as Significant Data Fiduciaries in the Bill), resembling the approach of the European Union and Singapore. The Bill also establishes supplementary obligations and safeguards

for the processing of personal data of children, following the model of the Singaporean data protection law. Further, provisions for cross-border data transfer, similar to those found in the European Union and Singapore, are also incorporated into the Bill. The Committee also appreciate the fact that by using the word “she” instead of “he”, for the first time, women have been acknowledged in any Central Act or Bill. The Committee are hopeful that the Bill while absorbing international practices would exemplify the best of the know-how to India and become a model legislation for the other countries to follow.

7. The Committee note that as of today, to protect personal data of users, the Central Government, in exercise of its powers under the Information Technology Act, 2000, has prescribed reasonable security practices and procedures for sensitive personal data or information through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. While these rules impose obligations on data collectors and processors to ensure reasonable security practices, the Committee recognize the need for a more comprehensive framework that delineate the rights and responsibilities of individuals whose digital personal data is involved, as well as the obligations of entities determining the purpose and methods of data processing. In order to strengthen personal data protection laws, the Government has developed and published a comprehensive legal framework known as the draft Digital Personal Data Protection Bill, 2022.

Further, due to the outdated nature of the Information Technology Act, enacted in 2000, the need for its substitution with the Digital India Act has become imminent. The Ministry is actively working on the Bill, which is expected to be rolled out in the near future. Recognizing the pressing need to fortify personal data protection laws, the introduction and subsequent implementation of the Digital India Bill becomes an imperative step forward. The Committee, therefore, strongly urge the Ministry to promptly finalize the framework of the Digital India Bill and expedite its enactment without any undue delay.



8. During the evidence the Committee were informed that the enactment of the Digital Personal Data Protection Bill necessitates amendments to certain provisions of the Information Technology Act, including Section 43A, Section 81, and Section 87. Even power of disclosure under Right to Information Act, which exempts from disclosure of personal information but empowers PIO/ Appellate Authority to disclose despite exemption has to be removed. The Committee urges the Ministry to proactively revisit the provisions of the Information Technology Act to ensure their congruence with the Constitutional spirit. The Committee further emphasize the need for bringing out subsequent amendments to other relevant acts, particularly the Information Technology Act, to complement the provisions outlined in the DPDP Bill.

**Ensuring robust safeguards for inclusive digital access through citizens' awareness:**

9. The Committee note that the safeguards proposed for processing of personal data of children include processing only with parental consent and not undertaking processing detrimental to children's well-being or involving tracking, behavioural monitoring or targeted advertising. However, to enable use in cases like protection of abandoned children, etc. The Committee have been apprised that the Ministry has made essential revisions to the draft, taking into account public feedback regarding the consideration of a child's maturity when determining the age of consent. Government may notify purposes where processing may be allowed without parental consent or with tracking, etc. The Committee further note that the Bill includes provisions that enable the establishment of prescribed methods for obtaining consent and delivering notices. As the Bill progresses, the consent and notice mechanisms may even incorporate visual elements, allowing for easier understanding and accessibility. The Committee urge the Ministry to incorporate these enabling provisions, so as to extend its benefits to digitally illiterate individuals, ensuring their inclusion in the evolving landscape of data privacy and protection.

The Committee are aware of the "Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA)" scheme that aims to usher in digital literacy in

rural India by covering 6 crore rural households (one person per household). To ensure equitable geographical reach, each of the 2,50,000 Gram Panchayats across the country are registering an average of 200-300 candidates. Special focus of the said Scheme is on training the beneficiaries on use of Electronic Payment System. As on 31st October, 2022, a total of 6.51 crore beneficiaries have been enrolled, out of which training has been imparted to 5.59 crore beneficiaries, out of this more than 4.15 crore beneficiaries have been certified under the PMGDISHA Scheme. The Committee recognize that the Scheme aims to bridge the digital divide, specifically targeting the rural population including the marginalised sections of society and is complementary to the Digital Personal Data Protection Bill which aims at inclusive governance.

The Committee therefore exhort the Ministry to put in all efforts in accelerating the progress of digital literacy while simultaneously aiming at a digitally safe cyber ecosystem for the citizens.

#### **Enhancing Citizen Awareness and Safeguarding Digital Personal Data:**

10. The Committee have been apprised during the deliberations that the Draft legislation to safeguard citizen's data security and privacy is slated to be introduced in the Parliament not only enhances the ease of doing business and ease of living but also enables speedier adjudication by providing for alternate dispute resolution and acceptance of voluntary undertakings by the adjudicatory body in an accountable manner. Further, any individual experiencing harm due to a civil wrong can seek compensation through torts law. This includes cases where a Data Fiduciary violates rights or fails to fulfill obligations. The affected person can bring a claim in a civil court and cite penalties imposed by the Board in support of his/her claim. The Committee strongly believe that ensuring public awareness on the mechanisms for alternative dispute resolution and remedies available in Civil Court is vital to protect citizens' interests. While acknowledging the provisions empowering individuals to exercise their rights over personal data, the Committee urge the Ministry to collaborate with State/UT Governments in organizing impactful

awareness campaigns. These campaigns should educate the public about alternative remedies in cases of harm caused by civil wrongs violating their rights. Additionally, there is a need to counsel and inform individuals about the option of Alternate Dispute Resolution through mediators. The Committee also suggest the establishment of a helpline number or online AI-based chatbot to provide guidance to affected individuals.

11. The Committee have been informed during the deliberation that draft Bill has a provision for robust consent mechanism and notice requirements regarding the usage of personal data. It emphasizes the importance of providing consent and notice in languages specified in the Eighth Schedule to the Constitution to ensure clarity and comprehension. It includes provisions that allow for the establishment of prescribed methods for obtaining consent and delivering notices. It also provides for Data Principals to have the right to withdraw their consent at any time. The Committee are pleased that it recognizes the need for the consent framework to adapt and improve over time for the processing of personal data. Therefore, the Committee urge the Ministry to ensure that the default consent settings are designed to extend benefits to data principals, especially digitally illiterate individuals. The Committee, further urge the Ministry to incorporate visual elements for consent and notice, promoting easier understanding, accessibility, and inclusive digital access while defining the prescribed methods for obtaining consent and delivering notices.

Further, to simplify the process and avoid the need to read the entire document containing terms and conditions, it would be beneficial to provide a summary or gist of the terms and conditions to the Data Principal. This would enable him/her to provide informed consent. The Committee are pleased to see that the it maintains enough flexibility to incorporate such a provision when establishing prescribed rules and are hopeful that the culturally and linguistically diverse population of India would benefit from an inclusive legislation.

**12. The Committee are pleased to note that the provision of the 'Deemed consent' clause, which was present in the draft Digital Personal Data Protection Bill, 2022 , has been removed based on public consultation and feedback from stakeholders. The personal data can now only be processed for certain legitimate uses. These exemptions are limited to the State and its instrumentalities to perform functions under law or in the interest of sovereignty and integrity of India and security of the State, to provide or issue subsidies, benefits, services, certificates, licences and permits that are prescribed through rules, to comply with any judgement or order under law, to protect or assist or provide service in a medical or health emergency, disaster situation or maintain public order and in relation to an employee.**

**While recognizing the right to privacy, the Supreme Court has also observed that privacy, like other fundamental rights, is not an absolute right. However, any law encroaching upon privacy must withstand the scrutiny of permissible restrictions on fundamental rights. Nevertheless, the Committee are of the view that there is still a possibility of these exceptions being misused. Therefore, the Committee strongly recommend the Ministry to devise a mechanism to ensure that these exceptions do not become the general rule and are used only in exceptional circumstances, with the aim of promoting ease of living and the digital economy.**

**13. The Committee note that a person who suffers a civil wrong on account of violation of her rights or non-compliance of obligations by a Data Fiduciary may raise such a claim before a civil court in consequence of such wrong. Such a person could also cite any penalty imposed by the Board for non-compliance as material in support of his/her claim. Further, as part of the deterrent mechanism, the Significant Data Fiduciary (SDF) in addition to the general obligations, will have to meet additional obligations like appointing India based data protection officer, conducting data protection impact assessment and data audit. In addition to these obligations, to make Data Fiduciaries accountable for the data processing, there are provision to impose financial penalty by data protection board in case of personal data breach by data fiduciaries after due inquiry under the principle of natural justice. The Bill entrusts entities to take reasonable**

security safeguards to prevent personal data breach with respect to the personal data in its possession making them accountable to the individuals. Further, if the Data Protection Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules by the entity is significant, it may, after giving the person an opportunity of being heard, impose monetary penalty. Also, the Central Government may, on the request of Board that intimates the imposition of monetary penalty on the entity in more than two instances and advises in the interests of the general public, instruct the appropriate agencies/intermediary to block the services of the entity.

The Committee note that like the data protection laws in the other mentioned jurisdictions, the Bill does not make any provision for any criminal liability, the liabilities envisaged are civil in nature. Although, criminal liability under certain sections of IPC like 405 may also be invoked in the case of data theft. The Committee are of the view that the criminal liability available under IPC may also be informed to the Public at large which would have a deterrent effect and fire fighting at a later stage would be avoided. Further, the Committee assert and recommend that publicising the same would discourage data theft.

14. The Committee note that the current draft of the Digital Personal Data Protection Bill, 2022 has been prepared with consideration for the dynamic nature of the subject matter. The threat landscape is constantly evolving at a rapid pace, requiring dynamic decision-making and the ability to adapt processes to counter these evolving threats. In order to address public concerns and provide sufficient adaptability, the draft Bill grants rule-making power to the Central government. The draft has been designed as technology-agnostic legislation to accommodate the rapid evolution of digital technology, which has significant social and economic impacts. Therefore, the law governing digital technology should possess the necessary flexibility to address changing situations and emerging requirements. While the Bill outlines the rights and duties of Data Principals and the obligations of Data Fiduciaries, it aims to retain sufficient flexibility to address these evolving needs.

The Committee are of the opinion that delegations of power are common in legislation and serve to make implementation practical and feasible. The Committee firmly believe that no legislation can be perfect from the outset. It evolves over time and is fine-tuned in response to changing circumstances. The Committee, therefore, urge that the provisions that cannot be fully defined within the scope of the Bill can be addressed through rules prescribed under the Bill, which are subsequently presented to Parliament. The Committee appreciate the wise step of making space for subordinate legislation, as it allows necessary flexibility to address changing situations and emerging requirements. However, the Committee also wish to caution the Ministry about the judicious use of rule-making powers and emphasizes the importance of employing them responsibly and with utmost care.

**Conclusion:**

15. In summation, the Committee, in no uncertain words stress the urgent necessity for the early enactment of a robust and all-encompassing legislation that effectively safeguards citizens' data and privacy. As the digital landscape continues to evolve rapidly, such legislation would serve as a crucial protective measure, ensuring the secure and responsible handling of personal information while instilling public confidence in the digital ecosystem. Delaying the implementation of such a comprehensive framework could potentially expose individuals to various risks and compromise the privacy rights of citizens. Hence, the Committee strongly advocate for the immediate action of enacting this crucial legislation to protect the interests and rights of citizens in the digital age. The Committee emphasize that the Observations and Recommendations put forth in this Report should be duly considered in the process.

New Delhi;  
...31....July, 2023  
...9.Sravana, 1945 (Saka)

PRATAPRAO JADHAV,  
Chairperson,  
Standing Committee on  
Communications and Information Technology.



<b>THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022</b>		
<b>Section No</b>	<b>Title</b>	<b>Page</b>
<b>CHAPTER 1: PRELIMINARY</b>		
<b>1</b>	<b>Short Title and Commencement</b>	<b>2</b>
<b>2</b>	<b>Definitions</b>	<b>2</b>
<b>3</b>	<b>Interpretation</b>	<b>5</b>
<b>4</b>	<b>Application of the Act</b>	<b>5</b>
<b>CHAPTER 2: OBLIGATIONS OF DATA FIDUCIARY</b>		
<b>5</b>	<b>Grounds for processing digital personal data</b>	<b>6</b>
<b>6</b>	<b>Notice</b>	<b>6</b>
<b>7</b>	<b>Consent</b>	<b>7</b>
<b>8</b>	<b>Deemed consent</b>	<b>9</b>
<b>9</b>	<b>General obligations of Data Fiduciary</b>	<b>10</b>
<b>10</b>	<b>Additional obligations in relation to processing of personal data of children</b>	<b>12</b>
<b>11</b>	<b>Additional obligations of Significant Data Fiduciary</b>	<b>13</b>
<b>Chapter 3: RIGHTS &amp; DUTIES OF DATA PRINCIPAL</b>		
<b>12</b>	<b>Right to information about personal data</b>	<b>14</b>
<b>13</b>	<b>Right to correction and erasure of personal data</b>	<b>14</b>
<b>14</b>	<b>Right of grievance redressal</b>	<b>14</b>
<b>15</b>	<b>Right to nominate</b>	<b>15</b>
<b>16</b>	<b>Duties of Data Principal</b>	<b>15</b>
<b>Chapter 4: SPECIAL PROVISIONS</b>		
<b>17</b>	<b>Transfer of personal data outside India</b>	<b>15</b>
<b>18</b>	<b>Exemptions</b>	<b>16</b>
<b>Chapter 5: COMPLIANCE FRAMEWORK</b>		
<b>19</b>	<b>Data Protection Board of India</b>	<b>17</b>
<b>20</b>	<b>Functions of the Board</b>	<b>17</b>
<b>21</b>	<b>Process to be followed by the Board to ensure compliance with the provisions of the Act</b>	<b>18</b>



22	Review and Appeal	19
23	Alternate Dispute Resolution	20
24	Voluntary Undertaking	20
25	Financial Penalty	20
<b>Chapter 6: MISCELLANEOUS</b>		
26	Power to make Rules	21
27	Power of Central Government to amend Schedules	22
28	Removal of difficulties	22
29	Consistency with other laws	22
30	Amendments	23
<b>Schedule 1</b>		<b>24</b>

## **THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022**

The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.

### **Chapter 1: PRELIMINARY**

#### **1. Short Title and Commencement**

- (1) This Act may be called the Digital Personal Data Protection Act, 2022.
- (2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint. Different dates may be appointed for different provisions of this Act. Any reference in any provision of this Act to the commencement of this Act shall be construed as a reference to the commencement of that provision.

#### **2. Definitions**

In this Act:—

- (1) “automated” means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data;

- (2) “Board” means the Data Protection Board of India established by the Central Government for the purposes of this Act;
- (3) “child” means an individual who has not completed eighteen years of age;
- (4) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;
- (5) “Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;
- (6) “Data Principal” means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child;
- (7) “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary;
- (8) “Data Protection Officer” means an individual appointed as such by a Significant Data Fiduciary under the provisions of this Act;
- (9) “gain” means-
  - (a) gain in property or a supply of services, whether temporary or permanent; or
  - (b) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.
- (10) “harm”, in relation to a Data Principal, means -
  - (a) any bodily harm; or
  - (b) distortion or theft of identity; or
  - (c) harassment; or
  - (d) prevention of lawful gain or causation of significant loss;
- (11) “loss” means –
  - (a) loss in property or interruption in supply of services, whether temporary or permanent; or
  - (b) a loss of an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.

- (12) “person” includes—
- (a) an individual;
  - (b) a Hindu Undivided Family;
  - (c) a company;
  - (d) a firm;
  - (e) an association of persons or a body of individuals, whether incorporated or not;
  - (f) the State; and
  - (g) every artificial juristic person, not falling within any of the preceding sub-clauses;
- (13) “personal data” means any data about an individual who is identifiable by or in relation to such data;
- (14) "personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
- (15) “prescribed” means prescribed by Rules made under the provisions of this Act;
- (16) “processing” in relation to personal data means an automated operation or set of operations performed on digital personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;
- (17) “proceeding” means any action taken by the Board under the provisions of this Act;
- (18) “public interest” means in the interest of any of the following:
- (a) sovereignty and integrity of India;
  - (b) security of the State;
  - (c) friendly relations with foreign States;
  - (d) maintenance of public order;
  - (e) preventing incitement to the commission of any cognizable offence relating to the preceding sub-clauses; and
  - (f) preventing dissemination of false statements of fact.

### **3. Interpretation**

In this Act: -

- (1) unless the context otherwise requires, a reference to “*provisions of this Act*” shall be read as including a reference to Rules made under this Act.
- (2) “*the option to access ... in English or any language specified in the Eighth Schedule to the Constitution of India*” shall mean that the Data Principal may select either English or any one of the languages specified in the Eighth Schedule to the Constitution of India;
- (3) the pronouns “her” and “she” have been used for an individual, irrespective of gender.

### **4. Application of the Act**

- (1) The provisions of this Act shall apply to the processing of digital personal data within the territory of India where:
  - (a) such personal data is collected from Data Principals online; and
  - (b) such personal data collected offline, is digitized.
- (2) The provisions of this Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India.

For the purpose of this sub-section, “profiling” means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal.

- (3) The provisions of this Act shall not apply to:
  - (a) non-automated processing of personal data;
  - (b) offline personal data;
  - (c) personal data processed by an individual for any personal or domestic purpose; and
  - (d) personal data about an individual that is contained in a record that has been in existence for at least 100 years.

## Chapter 2: OBLIGATIONS OF DATA FIDUCIARY

### 5. Grounds for processing digital personal data

A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder, for a lawful purpose for which the Data Principal has given or is deemed to have given her consent in accordance with the provisions of this Act.

For the purpose of this Act, “lawful purpose” means any purpose which is not expressly forbidden by law.

### 6. Notice

- (1) On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of processing of such personal data.
- (2) Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable.

For the purpose of this section: -

(a) “notice” can be a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected, or in such other form as may be prescribed.

(b) “itemised” means presented as a list of individual items.

**Illustration:** ‘A’ contacts a bank to open a regular savings account. The bank asks ‘A’ to furnish photocopies of proof of address and identity for KYC formalities. Before collecting the photocopies, the bank should give notice to ‘A’ stating that the purpose of obtaining the photocopies is completion of KYC formalities. The notice need not be a separate document. It can be printed on the form used for opening the savings bank account.

- (3) The Data Fiduciary shall give the Data Principal the option to access the information referred to in sub-sections (1) and (2) in English or any language specified in the Eighth Schedule to the Constitution of India.

## 7. Consent

- (1) Consent of the Data Principal means any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose.

For the purpose of this sub-section, "specified purpose" means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act.

- (2) Any part of consent referred in sub-section (1) which constitutes an infringement of provisions of this Act shall be invalid to the extent of such infringement.

*Illustration:* 'A' enters into a contract with 'B' to provide a service 'X' to 'B'. As part of the contract, 'B' consents to: (a) processing of her personal data by 'A', and (b) waive her right to file a complaint with the Board under the provisions of this Act. Part (b) of the consent by which 'B' has agreed to waive her right shall be considered invalid.

- (3) Every request for consent under the provisions of this Act shall be presented to the Data Principal in a clear and plain language, along with the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act. The Data Fiduciary shall give to the Data Principal the option to access such request for consent in English or any language specified in the Eighth Schedule to the Constitution of India.
- (4) Where consent given by the Data Principal is the basis of processing of personal data, the Data Principal shall have the right to withdraw her consent at any time. The consequences of such withdrawal shall be borne by such Data Principal. The withdrawal of consent shall not affect the lawfulness of processing of the personal data based on consent before its withdrawal. The ease of such withdrawal shall be comparable to the ease with which consent may be given.

*Illustration:* 'A' enters into a contract with 'B' to provide a service 'X' to 'B'. As part of the contract, 'B' consents to processing of her personal data by 'A'. If 'B' withdraws her consent to processing of her personal data, 'A' may stop offering the service 'X' to 'B'.

- (5) If a Data Principal withdraws her consent to the processing of personal data under sub-section (4), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing of the personal data of such Data Principal unless such processing without the Data Principal's consent is required or authorised under the provisions of this Act or any other law.

**Illustration:** 'A' subscribes to an e-mail and SMS-based sales notification service operated by 'B'. As part of the subscription contract, 'A' shares her personal data including mobile number and e-mail ID with 'B' which shares it further with 'C', a Data Processor for the purpose of sending alerts to 'A' via e-mail and SMS. If 'A' withdraws her consent to processing of her personal data, 'B' shall stop and cause 'C' to stop processing the personal data of 'A'.

- (6) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.

For the purpose of this section, a "Consent Manager" is a Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

- (7) The Consent Manager specified in this section shall be an entity that is accountable to the Data Principal and acts on behalf of the Data Principal. Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.
- (8) The performance of any contract already concluded between a Data Fiduciary and a Data Principal shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

**Illustration:** If 'A' enters into a contract with 'B' to provide a service 'X' to 'B' then 'A' shall not deny to provide service 'X' to 'B' on B's refusal to give consent for collection of additional personal data which is not necessary for the purpose of providing service 'X'.

- (9) Where consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by the Data Fiduciary to the Data Principal and consent was given by the Data Principal to the Data Fiduciary in accordance with the provisions of this Act.

## 8. Deemed consent

A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary:

- (1) in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data;

*Illustration: 'A' shares her name and mobile number with a Data Fiduciary for the purpose of reserving a table at a restaurant. 'A' shall be deemed to have given her consent to the collection of her name and mobile number by the Data Fiduciary for the purpose of confirming the reservation.*

- (2) for the performance of any function under any law, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State;

*Illustration: 'A' shares her name, mobile number and bank account number with a government department for direct credit of agricultural income support. 'A' shall be deemed to have given her consent to the processing of her name, mobile number and bank account number for the purpose of credit of fertilizer subsidy amount to her bank account.*

- (3) for compliance with any judgment or order issued under any law;
- (4) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;
- (5) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;
- (6) for taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order;
- (7) for the purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance;



**Illustration:** 'A' shares her biometric data with her employer 'B' for the purpose of marking A's attendance in the biometric attendance system installed at A's workplace. 'A' shall be deemed to have given her consent to the processing of her biometric data for the purpose of verification of her attendance.

- (8) in public interest, including for:
  - (a) prevention and detection of fraud;
  - (b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws;
  - (c) network and information security;
  - (d) credit scoring;
  - (e) operation of search engines for processing of publicly available personal data;
  - (f) processing of publicly available personal data; and
  - (g) recovery of debt;
  
- (9) for any fair and reasonable purpose as may be prescribed after taking into consideration:
  - (a) whether the legitimate interests of the Data Fiduciary in processing for that purpose outweigh any adverse effect on the rights of the Data Principal;
  - (b) any public interest in processing for that purpose; and
  - (c) the reasonable expectations of the Data Principal having regard to the context of the processing.

## **9. General obligations of Data Fiduciary**

- (1) A Data Fiduciary shall, irrespective of any agreement to the contrary, or non-compliance of a Data Principal with her duties specified in this Act, be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf by a Data Processor or another Data Fiduciary.

(2) A Data Fiduciary shall make reasonable efforts to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete, if the personal data:

(a) is likely to be used by the Data Fiduciary to make a decision that affects the Data Principal to whom the personal data relates; or

(b) is likely to be disclosed by the Data Fiduciary to another Data Fiduciary.

**Illustration:** *'A' has instructed her mobile service provider 'B' to mail physical copies of monthly bills to her postal address. Upon a change in her postal address, 'A' duly informs 'B' of her new postal address and completes necessary KYC formalities. 'B' should ensure that the postal address of 'A' is updated accurately in its records.*

(3) A Data Fiduciary shall implement appropriate technical and organizational measures to ensure effective adherence with the provisions of this Act.

(4) Every Data Fiduciary and Data Processor shall protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach.

(5) In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board and each affected Data Principal, in such form and manner as may be prescribed.

For the purpose of this section "affected Data Principal" means any Data Principal to whom any personal data affected by a personal data breach relates.

(6) A Data Fiduciary must cease to retain personal data, or remove the means by which the personal data can be associated with particular Data Principals, as soon as it is reasonable to assume that:

(a) the purpose for which such personal data was collected is no longer being served by its retention; and

(b) retention is no longer necessary for legal or business purposes.

**Illustration (A):** *'A' creates an account on 'X', a Social Media Platform. As part of the process of creating the account, 'A' shares her personal data with 'X'. After three months, 'A' deletes the account. Once 'A' deletes the account, 'X' must stop retaining the personal data of 'A' or remove the means by which the personal data of 'A' can be associated with 'A'.*

**Illustration (B):** 'A' opens a savings account with a bank. As part of KYC formalities, 'A' shares her personal data with the bank. After six months, 'A' closes the savings account with the bank. As per KYC rules, the bank is required to retain personal data for a period beyond six months. In this case, the bank may retain 'A's' personal data for the period prescribed in KYC Rules because such retention is necessary for a legal purpose.

- (7) Every Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the Data Principal's questions about the processing of her personal data.
- (8) Every Data Fiduciary shall have in place a procedure and effective mechanism to redress the grievances of Data Principals.
- (9) The Data Fiduciary may, where consent of the Data Principal has been obtained, share, transfer or transmit the personal data to any Data Fiduciary, or engage, appoint, use or involve a Data Processor to process personal data on its behalf, only under a valid contract. Such Data Processor may, if permitted under its contract with the Data Fiduciary, further engage, appoint, use, or involve another Data Processor in processing personal data only under a valid contract.

#### **10. Additional obligations in relation to processing of personal data of children**

- (1) The Data Fiduciary shall, before processing any personal data of a child, obtain verifiable parental consent in such manner as may be prescribed.

For the purpose of this section, "parental consent" includes the consent of lawful guardian, where applicable.

- (2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause harm to a child, as may be prescribed.
- (3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.
- (4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child for such purposes, as may be prescribed.

## **11. Additional obligations of Significant Data Fiduciary**

- (1) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including:
  - (a) the volume and sensitivity of personal data processed;
  - (b) risk of harm to the Data Principal;
  - (c) potential impact on the sovereignty and integrity of India;
  - (d) risk to electoral democracy;
  - (e) security of the State;
  - (f) public order; and
  - (g) such other factors as it may consider necessary;
  
- (2) The Significant Data Fiduciary shall:
  - (a) appoint a Data Protection Officer who shall represent the Significant Data Fiduciary under the provisions of this Act and be based in India. The Data Protection Officer shall be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary. The Data Protection officer shall be the point of contact for the grievance redressal mechanism under the provisions of this Act;
  - (b) appoint an Independent Data Auditor who shall evaluate the compliance of the Significant Data Fiduciary with provisions of this Act; and
  - (c) undertake such other measures including Data Protection Impact Assessment and periodic audit in relation to the objectives of this Act, as may be prescribed.

For the purpose of this section, “Data Protection Impact Assessment” means a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed.

### **Chapter 3: RIGHTS & DUTIES OF DATA PRINCIPAL**

#### **12. Right to information about personal data**

The Data Principal shall have the right to obtain from the Data Fiduciary:

- (1) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal;
- (2) a summary of the personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data Fiduciary with respect to the personal data of the Data Principal;
- (3) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and
- (4) any other information as may be prescribed.

#### **13. Right to correction and erasure of personal data**

- (1) A Data Principal shall have the right to correction and erasure of her personal data, in accordance with the applicable laws and in such manner as may be prescribed.
- (2) A Data Fiduciary shall, upon receiving a request for such correction and erasure from a Data Principal:
  - (a) correct a Data Principal's inaccurate or misleading personal data;
  - (b) complete a Data Principal's incomplete personal data;
  - (c) update a Data Principal's personal data;
  - (d) erase the personal data of a Data Principal that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.

#### **14. Right of grievance redressal**

- (1) A Data Principal shall have the right to readily available means of registering a grievance with a Data Fiduciary.

- (2) A Data Principal who is not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days or such shorter period as may be prescribed, may register a complaint with the Board in such manner as may be prescribed.

#### **15. Right to nominate.**

A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act.

For the purpose of this section, “incapacity” means inability to exercise the rights of the Data Principal under the provisions of this Act due to unsoundness of mind or body.

#### **16. Duties of Data Principal.**

- (1) A Data Principal shall comply with the provisions of all applicable laws while exercising rights under the provisions of this Act.
- (2) A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.
- (3) A Data Principal shall, under no circumstances including while applying for any document, service, unique identifier, proof of identity or proof of address, furnish any false particulars or suppress any material information or impersonate another person.
- (4) A Data Principal shall furnish only such information as is verifiably authentic while exercising the right to correction or erasure under the provisions of this Act.

### **Chapter 4: SPECIAL PROVISIONS**

#### **17. Transfer of personal data outside India**

The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.

## 18. Exemptions.

- (1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where:
  - (a) the processing of personal data is necessary for enforcing any legal right or claim;
  - (b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function;
  - (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law;
  - (d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India.
- (2) The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:
  - (a) by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and
  - (b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards specified by the Board.
- (3) The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply.
- (4) The provisions of sub-section (6) of section 9 of this Act shall not apply in respect of processing by the State or any instrumentality of the State.

## Chapter 5: COMPLIANCE FRAMEWORK

### 19. Data Protection Board of India

- (1) The Central Government shall, by notification, establish, for the purposes of this Act, a Board to be called the Data Protection Board of India. The allocation of work, receipt of complaints, formation of groups for hearing, pronouncement of decisions, and other functions of the Board shall be digital by design.
- (2) The strength and composition of the Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be such as may be prescribed.
- (3) The chief executive entrusted with the management of the affairs of the Board shall be such individual as the Central Government may appoint and terms and conditions of her service shall be such as the Central Government may determine.
- (4) The Board shall have such other officers and employees, with such terms and conditions of appointment and service, as may be prescribed.
- (5) The Chairperson, Members, officers and employees of the Board shall be deemed, when acting or purporting to act in pursuance of provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.
- (6) No suit, prosecution or other legal proceedings shall lie against the Board or its Chairperson, Member, employee or officer for anything which is done or intended to be done in good faith under the provisions of this Act.

### 20. Functions of the Board

- (1) The functions of the Board are:
  - (a) to determine non-compliance with provisions of this Act and impose penalty under the provisions of this Act; and
  - (b) to perform such functions as the Central Government may assign to the Board under the provisions of this Act or under any other law by an order published in the Official Gazette.
- (2) The Board may, for the discharge of its functions under the provisions of this Act, after giving a person, a reasonable opportunity of being heard and for reasons to be



recorded in writing, issue such directions from time to time as it may consider necessary, to such person, who shall be bound to comply with the same.

- (3) The Board may, in the event of a personal data breach, direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach or mitigate any harm caused to Data Principals.
- (4) The Board may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (2) and in doing so, may impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

**21. Process to be followed by the Board to ensure compliance with the provisions of the Act**

- (1) The Board shall function as an independent body and, as far as possible, function as a digital office and employ such techno-legal measures as may be prescribed.
- (2) The Board may, on receipt of a complaint made by an affected person or on a reference made to it by the Central Government or a State Government or in compliance with the directions of any court or in case of non-compliance with section 16 of this Act by a Data Principal, take action in accordance with the provisions of this Act.
- (3) The Board may authorise conduct of proceedings relating to complaints, by individual Members or groups of Members.
- (4) The Board shall first determine whether there are sufficient grounds to proceed with an inquiry. In case the Board determines that there are insufficient grounds, it may, for reasons recorded in writing, close such proceeding.
- (5) In case the Board determines that there are sufficient grounds to proceed with inquiry, it may, for reasons recorded in writing, inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the provisions of this Act.
- (6) The Board shall conduct such inquiry following the principles of natural justice including giving reasonable opportunity of being heard and shall record reasons for its actions during the course of such inquiry.

- (7) For the purpose of conduct of inquiry under this section, the Board shall have powers to summon and enforce the attendance of persons, examine them on oath and inspect any data, book, document, register, books of account or any other document.
- (8) Inquiry under this section shall be completed at the earliest. The Board or its officers shall not prevent access to any premises or take into custody any equipment or any item that may adversely affect the day-to-day functioning of a person.
- (9) The Board may require the services of any police officer or any officer of the Central Government or a State Government to assist it for the purposes of this section and it shall be the duty of every such officer to comply with such requisition.
- (10) During the course of the inquiry if the Board considers it necessary for preventing non-compliance with the provisions of this Act, it may, for reasons to be recorded in writing, issue interim orders after giving the concerned persons a reasonable opportunity of being heard.
- (11) On conclusion of the inquiry and after giving the concerned persons a reasonable opportunity of being heard, if the Board determines that non-compliance by a person is not significant, it may, for reasons recorded in writing, close such inquiry. If the Board determines that the non-compliance by the person is significant, it shall proceed in accordance with section 25 of this Act.
- (12) At any stage after receipt of a complaint, if the Board determines that the complaint is devoid of merit, it may issue a warning or impose costs on the complainant.
- (13) Every person shall be bound by the orders of the Board. Every order made by the Board shall be enforced by it as if it were a decree made by a Civil Court. For the purpose of this sub-section, the Board shall have all the powers of a Civil Court as provided in the Code of Civil Procedure, 1908.

## **22. Review and Appeal**

- (1) The Board may review its order, acting through a group for hearing larger than the group which held proceedings in a matter under section 21, on a representation made to it, or on its own, and for reasons to be recorded in writing, modify, suspend, withdraw or cancel any order issued under the provisions of this Act and in doing so, may impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

- (2) An appeal against any order of the Board shall lie to the High Court. Every appeal made under this section shall be preferred within a period of sixty days from the date of the order appealed against.
- (3) No civil court shall have the jurisdiction to entertain any suit or take any action in respect of any matter under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken under the provisions of this Act.

### **23. Alternate Dispute Resolution**

If the Board is of the opinion that any complaint may more appropriately be resolved by mediation or other process of dispute resolution, the Board may direct the concerned parties to attempt resolution of the dispute through mediation by a body or group of persons designated by the Board or such other process as the Board may consider fit.

### **24. Voluntary Undertaking**

- (1) The Board may accept a voluntary undertaking in respect of any matter related to compliance with provisions of this Act from any person at any stage.
- (2) Such voluntary undertaking may include an undertaking to take specified action within a specified time, an undertaking to refrain from taking specified action, and an undertaking to publicize the voluntary undertaking.
- (3) The Board may, after accepting the voluntary undertaking and with the agreement of the person who gave the voluntary undertaking vary the terms included in the voluntary undertaking. Acceptance of the voluntary undertaking by the Board shall constitute a bar on proceedings under the provisions of this Act as regards the contents of the voluntary undertaking, except in cases covered by sub-section (4).
- (4) Where a person fails to comply with any term of the voluntary undertaking accepted by the Board, the Board may, after giving such person, a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act.

### **25. Financial Penalty**

- (1) If the Board determines on conclusion of an inquiry that non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose such financial penalty as specified in Schedule 1, not exceeding rupees five hundred crore in each instance.

- (2) While determining the amount of a financial penalty to be imposed under sub-section (1), the Board shall have regard to the following matters:
- (a) the nature, gravity and duration of the non-compliance;
  - (b) the type and nature of the personal data affected by the non-compliance;
  - (c) repetitive nature of the non-compliance;
  - (d) whether the person, as a result of the non-compliance, has realized a gain or avoided any loss;
  - (e) whether the person took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;
  - (f) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the provisions of this Act; and
  - (g) the likely impact of the imposition of the financial penalty on the person.

## **Chapter 6: MISCELLANEOUS**

### **26. Power to make Rules**

- (1) The Central Government may, by notification make Rules consistent with the provisions of this Act to carry out the provisions of this Act.
- (2) Every Rule made under the provisions of this Act shall be laid as soon as may be after it is made, before each House of the Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form, or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

## **27. Power of Central Government to amend Schedules**

- (1) The Central Government may, by notification, amend Schedule 1 to this Act. No such notification shall have the effect of increasing a penalty specified in Schedule 1 to more than double of what was specified in Schedule 1 when this Act was originally enacted.
- (2) Any amendment notified under sub-section (1) shall have effect as if enacted in this Act and shall come into force on the date of the notification, unless the notification otherwise directs.
- (3) Every amendment made by the Central Government under sub-section (1) shall be laid as soon as may be after it is made, before each House of the Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the amendment or both Houses agree that the amendment should not be made, the amendment shall thereafter have effect only in such modified form, or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that amendment.

## **28. Removal of difficulties**

- (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, before expiry of five years from the date of commencement of this Act, by an order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the difficulty.
- (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

## **29. Consistency with other laws**

- (1) The provisions of this Act shall be in addition to, and not construed in derogation of the provisions of any other law, and shall be construed as consistent with such law, for the time being in force.
- (2) In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

**30. Amendments.**

- (1) The Information Technology Act, 2000 (“IT Act”) shall be amended in the following manner:
  - (a) section 43A of the IT Act shall be omitted;
  - (b) In section 81 of the IT Act, in the proviso, after the words and figures “the Patents Act, 1970”, the words “or the Digital Personal Data Protection Act, 2022” shall be inserted; and
  - (c) clause (ob) of sub-section (2) of section 87 of IT Act shall be omitted.
  
- (2) Clause (j) of sub-section (1) of section 8 of the Right to Information Act, 2005 shall be amended in the following manner:
  - (a) The words “the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information” shall be omitted;
  - (b) The proviso shall be omitted.

**Schedule 1**  
(See section 25)

Sl. No.	Subject matter of the non-compliance	Penalty
(1)	(2)	(3)
1	Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (4) of section 9 of this Act	Penalty up to Rs 250 crore
2	Failure to notify the Board and affected Data Principals in the event of a personal data breach, under sub-section (5) of section 9 of this Act	Penalty up to Rs 200 crore
3	Non-fulfilment of additional obligations in relation to Children; under section 10 of this Act	
4	Non-fulfilment of additional obligations of Significant Data Fiduciary; under section 11 of this Act	Penalty up to Rs 150 crore
5	Non-compliance with section 16 of this Act	Penalty up to Rs 10 thousand
6	Non-compliance with provisions of this Act other than those listed in (1) to (5) and any Rule made thereunder	Penalty up to Rs 50 crore

**Dr. JOHN BRITTAS**  
**MEMBER OF PARLIAMENT**  
**(RAJYA SABHA)**



**Member :**

- Standing Committee on Communications and Information Technology
- Consultative Committee for the Ministry of Information & Broadcasting
- Committee on Information and Communication Technology Management in Rajya Sabha

MPRS/07/1290/2023

28.07.2023

**The Chairman**

Department Related Parliamentary Standing Committee on Communications and Information Technology

Respected Chairman,

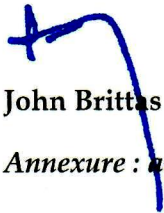
Sub:- 'Citizens' data security and privacy- 'Digital Personal Data Protection Bill' - Consideration and adoption of Report - dissent note - reg:

Kind attention is invited to the captioned subject.

Please recollect the fact that I had placed my Note of Dissent on 26.07.2023 during the sitting of the Department Related Parliamentary Standing Committee on Communications and Information Technology expressing my reservations over the captioned Report taken for consideration and adoption by the Committee, before boycotting the meeting protesting over the illegalities. As it has been requested that the dissent note be sent on e-mail, I hereby despatch the same and the same may kindly be treated as part of the Report of the Committee as per Rule 331 I (3) of the Rules of Procedure and Conduct of Business in Lok Sabha and Rule 274(3) of the Rules of Procedure and Conduct of Business in the Council of States (Rajya Sabha).

Thanking you.

Yours faithfully,

  
**John Brittas**

*Annexure : as above*



**Dr. JOHN BRITTAS**  
**MEMBER OF PARLIAMENT**  
**(RAJYA SABHA)**



**Member :**

- Standing Committee on Communications and Information Technology
- Consultative Committee for the Ministry of Information & Broadcasting
- Committee on Information and Communication Technology Management in Rajya Sabha

### NOTE OF DISSENT

1. It is imperative to note that the 'Digital Personal Data Protection Bill' had neither been introduced before either of the Houses of Parliament till date, nor was it referred to the Standing Committee by the Chairman of the Rajya Sabha or the Speaker, as the case may be, for examination.
2. According to the unequivocal provisions in Rules 331E (1) (b), 331H (a) & 331H (b) of Lok Sabha Rules and Rules 270 (b) & 273 (a) of the Rajya Sabha Rules, the Standing Committees are explicitly prohibited from examining any Bills that have not been referred to them by the Chairman or the Speaker after their introduction in either House.
3. Hence, it is evident that the above mentioned draft Report of the Standing Committee on Communications and Information Technology, containing Report on the examination and Recommendations of the Committee on the 'Digital Personal Data Protection Bill' are *void ab initio* and are *ultra vires* of the powers of the Standing Committee conferred by the Rules. The Rules proscribe the Standing Committee from examining such yet to be introduced Bills.

Without prejudice to the above, the following Note of Dissent vis-a-vis the draft Report presented to the Committee may also be recorded.

#### **Note of dissent on the Recommendations in the draft Report titled as "Citizens' data security and privacy" about the "Digital Personal Data Protection Bill"**

4. There is excessive delegated legislation in the proposed **Digital Personal Data Protection Bill**, as the draft bill does not go into the specifics of the implementation. It seems as if the Government's favourite catchphrase "as may be prescribed" is the highlight of this draft bill. It has been mentioned 18 times in a 24 page bill with only 30 clauses.
5. The proposed Bill gives Union Government unfettered power to give exemptions to government agencies [clause 18(2)] from the application of provisions of the Bill on specified grounds like sovereignty and integrity of India, friendly relations with foreign States, public order etc.
6. Additionally, clause 18(3) allows the Government to exempt any Data Fiduciary or a class of Data Fiduciary from the application of this proposed Act. Such sweeping exemptions raises major concerns like-
  - a. Whether it will meet the proportionality test set out by Supreme Court in the K.S. Puttaswamy Judgement (2017)? Will it not lead to violation of fundamental right to privacy?

Office (Delhi) : 140, South Avenue, New Delhi - 110 011, PH: 011 - 23792800, Mobile: +91 - 98477 20010

Office (Kerala) : Kairali Towers, Asan Square, University (P.O.), Palayam, Thiruvananthapuram, Kerala - 695 034, PH: 0471 - 2386556, 2386500  
E-mail: john.brittass@sansad.nic.in, johnbrittassmp@gmail.com



**Dr. JOHN BRITTAS**  
**MEMBER OF PARLIAMENT**  
**(RAJYA SABHA)**



**Member :**

- Standing Committee on Communications and Information Technology
- Consultative Committee for the Ministry of Information & Broadcasting
- Committee on Information and Communication Technology Management in Rajya Sabha

- b. It will lead to an untoward situation where any Data Fiduciary or any class of Fiduciaries would be able to exert pressure for seeking permission for exemption from the Act.
7. The proposed Data Protection Board of India is at the risk of becoming a puppet of the Centre, because everything ranging from composition, qualifications, tenure and procedure of appointment of members would be as per the whims and fancies of the Government.
  - a. The Joint Parliamentary Committee Report on the Personal Data Protection Bill, 2019 had recommended that a Selection Committee shall nominate the Data protection Authority. Members of the Committee itself should include: (i) Attorney General of India, (ii) an independent expert from fields such as data protection, information technology, or cyber laws, and (iii) Directors of an IIT and an IIM. None of this has been touched upon in the 2022 draft.
8. The bill does not include non-digital personal data, anonymized personal data, and non-personal data in its ambit, thus no protection is available to these kinds of data. It goes against the recommendations of the Joint Parliamentary committee on the Personal Data Protection Bill, 2019.
9. The Bill does not provide for the Right to data portability and the Right to be forgotten. The 2019 Bill on Data Protection and the Joint Parliamentary Committee, examining the 2019 Bill, recommended retaining these rights. The GDPR of EU also recognises these rights.
10. The bill removes the distinction between sensitive and critical personal data. This distinction was recommended by Justice Srikrishna and was included in the Personal Data Protection Bill, 2019 and the Joint Parliamentary Committee recommendations.
11. The draft bill no longer requires local storage of data. Businesses can only transfer data to countries notified by the Indian govt. During the examination of Ministry officials before the committee, it was deposed that a 'negative list' or a list of disapproved countries will be notified and cross-border data transfers to countries not on 'negative list' will be allowed on default basis. Without the assessment criteria being defined in the Digital Personal Data Protection Bill for such 'negative list', it could depend more on geopolitics than privacy safeguards.
12. Clause 24 of the draft bill talks about 'Voluntary Undertaking', under which the Data Protection Board has powers to accept voluntary undertaking with respect to non-compliance with any provisions of the proposed Act. Such a provision allows those who are non-compliant to avoid penalties ranging up to rupees 500 crore by giving a mere undertaking. The bill should clearly state the mechanism which the Data Protection Board would employ to accept such an undertaking.



**Dr. JOHN BRITTAS**  
**MEMBER OF PARLIAMENT**  
**(RAJYA SABHA)**



Member :

- Standing Committee on Communications and Information Technology
- Consultative Committee for the Ministry of Information & Broadcasting
- Committee on Information and Communication Technology Management in Rajya Sabha

13. While the Data Protection Board of India has the power to impose penalty on a Data Fiduciary for breach of personal data as per the Bill, it is not given the power to provide compensation to the aggrieved Data Principals. On the other hand, it is surprising to see that the Bill proposes a penalty of up to Rs 10,000 for Data Principals, in case, he/she fails to comply with section 16 of the Bill (Duties of Data Principal).
14. The Bill [as per clause 30(1)(a)] amends the IT act, 2000 and proposes to omit section 43A of the IT act. Section 43(A) of the IT Act, 2000 enables an aggrieved person to demand compensation from a body corporate due to any negligence in handling any sensitive personal data, thereby causing wrongful loss or wrongful gain to any person. This further accentuates the precarious situation of Data Principals. The GDPR of EU, on the other hand, specifically provides for Right to compensation to an aggrieved party under Article 82 for damage caused as a result of an infringement of the provisions of the regulation.
15. Section 8(1)(j) of the RTI act allows personal information to be disclosed if the larger public interest justifies the disclosure of such information (subject to satisfaction of Central Public Information Officer or the State Public Information Officer or the appellate authority), or it is related to any public activity or interest; even if the disclosure causes unwarranted invasion of the privacy of the individual, or if it is such an information which cannot be denied to the Parliament or a State Legislature. These portions are proposed to be deleted vide section 30(2) of the new Digital personal Data Protection Bill making all personal information exempt from RTI Act. This would fundamentally weaken the RTI Act and adversely impact the ability of people to access information and will definitely curtail transparency in the Government.
16. Notice requirements weakened: Compared to past versions, data fiduciaries do not have to inform principals about the third-parties with whom their data will be shared, the duration for which their data will be stored and if their data will be transferred to other countries.
17. Vague non-consensual processing of data permitted: The DPDPB, 2022 allows the Data Fiduciary to “deem” or assume consent of the Data Principal if the processing is considered necessary as per certain situations such as for the breakdown of public order, for purposes related to employment, and in public interest.

  
**John Brittas**

**STANDING COMMITTEE ON COMMUNICATIONS AND  
INFORMATION TECHNOLOGY (2022-23)**

**MINUTES OF THE FOURTH SITTING OF THE COMMITTEE**

-----

The Committee sat on Friday, the 2<sup>nd</sup> December, 2022 from 1130 hours to 1325 hours in Committee Room No. '3', Extension to Parliament House Annexe, New Delhi.

**PRESENT**

**Shri Prataprao Jadhav - Chairperson**

**MEMBERS**

**Lok Sabha**

2. Shri Karti P. Chidambaram
3. Dr. Nishikant Dubey
4. Shri P.R. Natarajan
5. Shri Sanjay Seth

**Rajya Sabha**

6. Dr. Anil Agrawal
7. Dr. John Brittas
8. Shri Kartikeya Sharma
9. Shri Jawhar Sircar
10. Shri Lahar Singh Siroya

**Secretariat**

- |                        |   |                 |
|------------------------|---|-----------------|
| 1. Shri Satpal Gulati  | - | Joint Secretary |
| 2. Smt. A. Jyothirmayi | - | Director        |

## **List of Witnesses**

### **Ministry of Electronics and Information Technology (MeitY)**

<b>Sl. No.</b>	<b>Name</b>	<b>Designation</b>
1.	Shri Alkesh Kumar Sharma	Secretary
2.	Shri Amit Agrawal	Additional Secretary
3.	Shri Deepak Goel	Scientist 'E' & GC
4.	Dr. Sanjay Bahl	DG, CERT-In
5.	Shri Rakesh Maheshwari	Scientist 'G' & GC (Parliament)
6.	Smt. Savita Utreja	Scientist 'E'
7.	Shri Vikas Chourasia	Scientist 'C'

2. At the outset, the Chairperson welcomed the Members to the sitting of the Committee. Members were informed that the Sitting had been convened to hear the views of representatives of MeitY on the subject 'Citizens' data security and privacy'.

[The representatives of MeitY were then called in]

3. The Chairperson welcomed the representatives of MeitY to the sitting of the Committee. The representatives of MeitY made a power-point presentation on the subject.

4. The presentation covered the global scenario on citizens' data security and privacy, the design principles for the draft Digital Personal Data Protection Bill, 2022, the international best practices adopted in the draft bill, the objectives, key definitions and applicability of the draft bill, the grounds for processing digital personal data, provision of deemed consent, general obligations of data fiduciary including additional obligations for processing childrens' data, Right to information about personal data, right

to correction and erasure of personal data, rights of grievance redressal and nomination, duties of data principal, trans-border movement of personal data, exemptions, compliance framework, consistency with other laws, amendments of other Acts and simple and direct language of the draft bill and so on.

5. Thereafter, Members raised queries on various issues such as the existing data security and privacy framework in the country, inherent gaps in the existing data security and privacy framework, key changes made in the draft 'Digital Personal Data Protection Bill, 2022' *vis-à-vis* the erstwhile withdrawn 'Personal Data Protection Bill, 2019', how the new Bill sought to fill-up those gaps and how the current draft Bill measured up to the prevalent global standard practices in the domain of data security and privacy. Some of the key issues discussed inter-alia included:-

- Lack of clear cut distinction between personal and non-personal data.
- Consent forms which compulsorily forced mobile App users to give blanket permissions.
- Need for distinction between personal v/s non-personal & digital v/s analog data instead of having a common 'Data Protection Act'.
- Whether the draft Bill was in consonance with the Supreme Court judgment in Justice Puttaswamy case.
- Provision for withdrawal of deemed consent.
- Right to be forgotten and Right to erasure.
- Balancing between Privacy v/s Surveillance
- The reasons for no public disclosure of submissions received on the draft Bill from general public.
- Provision of pervasive power to the Executive for delegated legislation.
- Provision of blanket exemption to large data fiduciaries.
- Dilution of data protection board.
- Lack of clarity on grounds for a complaint to be deemed frivolous.

6. Queries on privacy of personal information on social networking websites, the recently reported data security breach at the All India Institute of Medical Sciences (AIIMS), and impact of lack of a comprehensive data protection law in dealing with such

incidents were also raised. Representatives sought permission to send the replies in writing.

7. Taking the discussion further, the Committee desired to know the chronology of events which have led to the evolution of the draft Digital Personal Data Protection Bill, 2022 in its present form, the key issues addressed in the draft Bill, the consultation process to be followed and the timeframe within which the Bill is expected to be enacted. The Committee also wished to be apprised of the repercussions of the proposed draft Digital Personal Data Protection Bill, 2022 on the existing Information Technology Act and the Aadhaar Act and how the proposed bill would deal with issues such as ownership of data, localization of data, penal provisions for breach of privacy, non-consensual use of data by the State, safeguards against large scale State surveillance etc., to which the representatives of the Ministry responded.

8. The Chairperson, then, thanked the representatives of MeitY for deposing before the Committee and directed that written replies to points on which information was not readily available may be furnished to the Committee within a period of ten days.

The witnesses then withdrew  
Verbatim proceedings of the sitting have been kept on record.

**The Committee, then, adjourned.**

\*\*\*\*\*

**MINUTES OF THE FIFTEENTH SITTING OF THE STANDING  
COMMITTEE ON COMMUNICATIONS AND INFORMATION  
TECHNOLOGY (2022-23) HELD ON 15<sup>th</sup> JUNE, 2023**

-----

The Committee sat on Thursday, the 15<sup>th</sup> June, 2023 from 1130 hours to 1325 hours in Committee Room 'C', Parliament House Annexe, New Delhi.

**PRESENT**

**Shri Prataprao Jadhav – Chairperson**

**MEMBERS**

*Lok Sabha*

2. Dr. Nishikant Dubey
3. Shri Karti P. Chidambaram
4. Smt. Raksha Nikhil Khadse
5. Shri P.R. Natarajan
6. Shri Santosh Pandey
7. Shri Ganesh Singh
8. Shri Parvesh Sahib Singh
9. Shri Shatrughan Prasad Sinha
10. Shri L.S. Tejasvi Surya



### ***Rajya Sabha***

11. Dr. Anil Agrawal
12. Shri Jaggesh
13. Shri Kartikeya Sharma
14. Shri Jawhar Sircar
15. Shri Lahar Singh Siroya

### ***SECRETARIAT***

1. Shri Satpal Gulati - Joint Secretary
2. Shri Nishant Mehra - Deputy Secretary

### **Representatives of the Ministry of Electronics and Information Technology**

<b>Sl. No.</b>	<b>Name</b>	<b>Designation</b>
1.	Shri Alkesh Kumar Sharma	Secretary
2.	Shri Amit Agrawal	Additional Secretary
3.	Dr. Sandip Chatterjee	Scientist 'G' and Group Coordinator
4.	Shri Deepak Goel	DDG, NIC
5.	Ms. Tulika Pandey	Scientist 'G' and Group Coordinator

6. Shri Vishal Chauhan JS(Policy), M/o Health & Family Welfare
7. Shri Vikash Chourasia Scientist 'C'

2. At the onset of the Sitting, the Chairperson welcomed the representatives of the Ministry. In his welcome address, he emphasized that the protection of citizens' data security and privacy is essential for the functioning of a democratic society and the preservation of our fundamental values. He stressed that the consequences of a data breach can be devastating, leading to identity theft, financial loss, reputational damage, and even psychological distress. He mentioned that the Ministry had rolled out an improved version of "The Digital Personal Data Protection Bill, 2022" which recognized both the right of individuals to protect their personal data and the need to process personal data for lawful purposes. He further highlighted that when citizens' privacy is compromised, it erodes trust in the Institutions and Organizations that collect and handle our data and therefore, citizens must have the power to determine how their data is shared without excessive surveillance or profiling .

3. The Chairperson further asked the Ministry to apprise the Committee of the steps taken to strengthen legal frameworks and regulations that govern data protection and privacy, whether the proposed Bill spelt out clear guidelines for data collection, storage, and usage with strong penalties for those who violate these rules and how far decriminalizing violations would have an impact on compliance. He further asked about the steps taken by the Ministry towards garnering International cooperation and coordination, as data flows across borders and global standards need to be established to protect citizens' data privacy on a global scale.

4. After the welcome address by the Chairperson, the representatives of the Ministry of Electronics and Information Technology made a power-point presentation covering various aspects such as background of the Digital Personal Data Protection Bill, growing use of digital personal data necessitating focussed law to protect it, declaration of right to privacy as part of the Fundamental Rights in the Puttaswamy case. It mentioned the aims of the Bill which included introducing data protection law with minimum disruption while ensuring necessary change in the way Data Fiduciaries process data, to enhance ease of living and ease of doing business, to create a future ready, evolvable framework of trust, data protection and digital trade and to enable India's digital economy and its innovation ecosystem. They underlined the principles of the Bill as consented, lawful and transparent use of personal data, purpose and storage limitation, data minimization and pointed out that the bill used the pronoun 'she' instead of 'he' for the first time in a Central legislation.

5. The presentation also covered the focus of the Bill on minimizing disruption with the data fiduciary processing data on existing consent to notify the data principal, while continuing to do processing unless consent is withdrawn and permitting data processing outside India with India retaining the right to restrict processing in notified countries. It further highlighted that the Bill contained provisions for alternate dispute resolution and voluntary undertakings for faster resolution, accountability through monetary penalty without criminal offence and taking the data principal's consent in any 8<sup>th</sup> Schedule language. The presentation brought out that the Bill was not applicable to processing of personal data made publicly available by the Data principal herself, made publicly available by law and for personal or domestic purpose. The presentation specified that consent can be withdrawn at any time with consent managers accountable to data principals through an accessible, transparent and interoperable platform. The Committee were

also informed about the legitimate uses of data, obligations of data fiduciaries, processing of children's data for notified purposes, rights and duties of data principal, functions of data protection board and consistency with other laws.

6. Thereafter, Members sought clarification on various issues as follows-

- (i) specified purpose of storage and processing of data and deletion afterwards
- (ii) usage of data for national security, providing subsidies, medical emergencies, disaster management etc.
- (iii) restriction of certain countries from accessing data of Indian nationals
- (iv) functioning of data protection board and appellate tribunal
- (v) summary consent in the languages of the Eighth schedule
- (vi) withdrawal of consent and consequent erasure of data
- (vii) data protection impact assessment
- (viii) fast track mechanism for breach of the law
- (ix) time and purpose limitation of consent ( auto lapsability )
- (x) securing data of the digitally illiterate, children and the differently abled
- (xi) criminal liabilities of data fiduciaries in case of breach

7. Members also raised queries relating to protection of data in case of merger or demerger, digital literacy achieved by PMGDisha, right to be forgotten which were responded to by the representatives of the Ministry. Members also sought inputs on the appellate mechanism in the Bill. The Ministry assured the Committee to revisit the provisions of the draft Bill based on the feedback, concerns and suggestions made by the Committee.

8. The Chairperson, then, thanked the representatives of the Ministry for deposing before the Committee and asked them to send the replies to the unanswered queries within ten days.

The witnesses then withdrew.

Verbatim Proceedings of the Sitting have been kept on record.

**The Committee, then, adjourned.**

\*\*\*\*\*

**STANDING COMMITTEE ON COMMUNICATIONS AND INFORMATION  
TECHNOLOGY  
(2022-23)**

**MINUTES OF THE SIXTEENTH SITTING OF THE COMMITTEE**  
-----

The Committee sat on Wednesday, the 26<sup>th</sup> July, 2023 from 1000 hours to 1055 hours in Committee Room 'D', Parliament House Annexe, New Delhi.

**PRESENT**  
**Shri Prataprao Jadhav**

**MEMBERS**

***Lok Sabha***

2. Shri Karti P. Chidambaram
3. Shri Nishikant Dubey
4. Shri Santosh Pandey
5. Shri Sanjay Seth
6. Dr. T. Sumathy (A) Thamizhachi Thangapandian
7. Smt. Raksha Nikhil Khadse
8. Dr. Sukanta Majumdar
9. Ms. Mahua Moitra
10. Shri P.R. Natarajan
11. Shri Shatrughan Prasad Sinha
12. Dr. M. K. Vishnu Prasad
13. Shri Jayadev Galla

***Rajya Sabha***

14. Dr. Anil Aggarwal
15. Dr. John Brittas
16. Shri Syed Nasir Hussain
17. Shri Kartikeya Sharma
18. Shri Jawahar Sircar
19. Shri Lahar Singh Siroya
20. Shri Jaggesh
21. Shri Praful Patel

## **SECRETARIAT**

- |                        |   |                  |
|------------------------|---|------------------|
| 1. Shri Satpal Gulati  | - | Joint Secretary  |
| 2. Smt. A. Jyothirmayi | - | Director         |
| 3. Shri Nishant Mehra  | - | Deputy Secretary |

2. At the outset, the Chairperson welcomed the Members to the Sitting of the Committee convened to consider and adopt two Draft subject Reports relating to the Ministries/Departments under their jurisdiction.

3. The Committee, then, took up the following draft Reports for consideration and adoption.

- (i) Draft Report on “Citizens’ data security and privacy” related to Ministry of Electronics and Information Technology.
- (ii) Draft Report on “Review of functioning of Central Board of Film Certification (CBFC)” related to Ministry of Information and Broadcasting.

4. After due deliberations, the Committee adopted the draft Report on “Review of functioning of Central Board of Film Certification (CBFC)” with modifications.

5. As regards the draft Report on “Citizens’ data security and privacy” , some Members pointed out the Rule 331 H of the Rules of Procedure and Conduct of Business in Lok Sabha which *inter alia* states that the Committee shall consider only such Bills introduced in either of the Houses as are referred to them by the Chairman, Rajya Sabha or the Speaker, as the case may be and stated that the Draft Personal Data Protection Bill, 2023 had not been referred to the Committee. They also placed on record their disagreement with the Report which examined the Clauses of the said Bill. Some Members insisted that a division of votes may be conducted to determine the majority which was eventually not implemented. Further, some Members left the Sitting saying that a Whip had been issued to them to attend the House and some others left saying that the Report cannot be submitted to the Parliament as the Bill had not been referred to the Committee. One of the Members stated that he was submitting a dissent Note and the same was to be appended to the Report.

6. At the end of the Sitting, the Chairperson said that the Report was adopted. The remaining Members of the Committee authorized the Chairperson to finalize the draft Reports arising out of factual verification, if any, and present the Reports to the House during the current Session of Parliament.

**The Committee, then, adjourned.**