INTERNET FREEDOM FOUNDATION

Public Brief on

INDIA'S DIGITAL PERSONAL DATA PROTECTION FRAMEWORK

December, 2025
First Edition

Internet Freedom Foundation

I-1718, Third Floor, Chittaranjan Park, New Delhi 110019

Internet Freedom Foundation (“IFF”) is a registered charitable trust that works to advance constitutional guarantees in India, especially as they relate to digital rights and freedoms, through strategic litigation, government engagement, and civic advocacy. We work across a wide spectrum of issues, with expertise in free speech, platform governance, electronic surveillance, data protection, net neutrality, innovation and emerging technologies.

Recommended Citation: Indumugi C., Naman Kumar, and Avanti Deshpande, “Public Brief on India’s Digital Personal Data Protection Framework", (Internet Freedom Foundation, 22 December 2025).

Authors:

Indumugi C. is an Advocate based in New Delhi, and retained as a Legal Counsel at the Internet Freedom Foundation. She has prior experience in regulatory litigation and investor-state dispute settlement. Her interests include labour law, legal mobilization, and public law.

Naman Kumar is an Advocate based in New Delhi and retained as a Counsel at the Internet Freedom Foundation. His work at IFF focuses on the right to be forgotten, platform governance, digital rights, data protection, as well as broadcasting and telecommunication laws.

Avanti Deshpande is an Advocate based in New Delhi, and retained as a Counsel at the Internet Freedom Foundation. Her interests include digital rights, criminal justice, and issues at the intersection of law and gender.

Published: 22 December 2025

INTERNET FREEDOM FOUNDATION

Dear friends,

For over eight years, IFF has been at the frontlines, advocating for a data protection framework that truly serves Indians, rather than just the interests of the State or the bottom lines of corporations. With the notification of the Digital Personal Data Protection (DPDP) Act, 2023, and its subsequent Rules in late 2025, India has finally entered its era of statutory data regulation. However, as the dust settles on the legislative process, a concerning trend has emerged in the public discourse. Most analyses you will find today are written through the narrow lens of corporate compliance answering questions on implementation costs and penalties for breaches. While these are valid questions for the private sector, they often ignore the more profound, structural shifts this law imposes on our democracy.

This is why we are sharing this Public Brief. Our aim is not just to provide a sterile legal breakdown of the DPDP Act's provisions, but to offer an understanding of how these laws will actually impact civil society in India. The core of our concern, and the focus of this brief, lies in how the DPDP Act alters the relationship between the citizen and the State. While much has been said about "notice and consent" for apps and websites, this brief dives deep into the sweeping exemptions granted to the government. Crucially, we look at the impact on Civil Society Organizations (CSOs). For decades, non-profits have acted as trusted intermediaries for the most vulnerable. Under this new regime, these organizations are being pressured to become data gathering arms of the State. The compliance burden meant for tech giants is now a weight on small grassroots groups, potentially forcing them to collect more identity documents than ever before just to stay on the right side of the law.

This brief also unpacks the silencing effect on transparency. We look at the amendments to the RTI Act and the lack of journalistic exemptions, which threaten to turn a law meant for "protection" into a shield for "opacity". At IFF, we believe that privacy is not a luxury for the elite and needs to be realised as a fundamental prerequisite for a functioning democracy. We hope this brief serves as a guide for advocates, journalists, and citizens to navigate this new legal landscape and continue the fight for digital rights. I wish to compliment my colleagues, IFF's Counsels, Avanti, Indu, and Naman for their work. We encourage you to write back to us on policy@internetfreedom.in if you are working on issues of human rights, or any journalists with any queries or requests for help. As a public organisation, we are always happy to offer support which includes press requests, pro-bono legal support, advice and training based on our limited capacity.

Apar Gupta
Founder Director,
Internet Freedom Foundation

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Term	Abbreviation
Digital Personal Data Protection Act, 2023	DPDP Act
The Data Protection Bill, 2021	DPB, 2021
Data Protection Board	DPB/Board
Digital Personal Data Protection Bill, 2022	DPDPB, 2022
Digital Personal Data Protection Bill, 2023	DPDPB, 2023
Digital Personal Data Protection Rules, 2025	DPDP Rules
Data Protection Impact Assessment	DPIA
Data Protection Officer	DPO
General Data Protection Regulation	GDPR
Joint Parliamentary Committee	JPC
Ministry for Electronics and Information Technology	MeitY
Significant Data Fiduciary	SDF
The Personal Data Protection Bill, 2019	PDPB, 2019
The Right to Information Act, 2005	RTI Act

I. LEGISLATIVE HISTORY

1. Present status and timeline for implementation

On 11 August 2023, the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") received assent from the President of India.[1] On 13 November 2025, the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") were published in the gazette.[2] The timelines set by the Central Government for implementing the DPDP Act and DPDP Rules are as follows:

Date effective	DPDP Act[3]	DPDP Rules[4]	Content
13 November 2025	Sections 1(2), 2, 18-26, 35, 38-43, 44(1), and 44(3)	Rules 1, 2, and 17	• Data Protection Board • Power to make rules • Amendments to TRAI Act • Amendments to RTI Act
13 November 2026	Sections 6(9) and 27(1)(d)	Rule 4	• Registration of Consent Managers
13 May 2027	Sections 3-5, 6(1)-6(8), 6(10), 7-10, 11-17, 27 (besides 27(1)(d)), 28-34, 36-37, and 44(2)	Rules 3, 5 to 16, 22 and 23	• Obligations of Data Fiduciaries • Rights and duties of Data Principals • Powers, functions, and procedures of the Data Protection Board, appeal and dispute resolution • Power to call for information • Power of Central Government to issue directions

[1] Digital Personal Data Protection Act, 2023 ["DPDP Act"].
[2] Digital Personal Data Protection Rules, 2025 ["DPDP Rules"].
[3] MeitY, Gazette Notification dated 13 November 2025, F. No. AA-11038/1/2025-CL&ES, available at: https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf.
[4] DPDP Rules, s. 1.

2. Past efforts by the Government

Previous versions of a Data Privacy Bill have been coordinated through the Ministry of Personnel, Public Grievances, and Pensions since 2011.[5] Drafts of that bill dealt with both data protection and surveillance reform till 2014; however, it did not proceed further.[6] An Expert Committee on Privacy headed by Justice A.P. Shah under the erstwhile Planning Commission presented a report on 12 October 2012 which serves as an influential document on international & national privacy standards.[7] The Expert Committee on Data Protection chaired by Justice BN Srikrishna was constituted by the Ministry for Electronics and Information Technology ("**MeitY**") on 31 July 2017.[8] The ten-member Committee's mandate was to examine issues related to data protection, recommend methods to address them, and draft a data protection bill. It was criticised for its flawed composition and issues of conflict of interest.[9] The Committee released its 176 page Report to the MeitY and proposed the Personal Data Protection Bill, 2018 on 27 July 2018.[10]

As soon as the Personal Data Protection Bill, 2019 ("**PDPB, 2019**") was introduced in the Parliament on December 11, 2019, it was sent to a Joint Parliamentary Committee ("**JPC**") with members from both the Houses for its review and suggestions.[11] After nearly two years and several extensions, the Joint Committee on the Personal Data Protection Bill, 2019 brought out its report on December 16, 2021.[12] The Report also contained a new version of the law titled, 'The Data Protection Bill, 2021' ("**DPB, 2021**"). However, the DPB, 2021 was withdrawn by the Minister for Communications and Information Technology, Ashwini Vaishnaw on 03 August 2022.[13] On 18 November 2022, the MeitY published the draft 'Digital Personal Data Protection Bill, 2022' ("**DPDPB, 2022**"), along with an explanatory note, and

---

[5] Ministry of Personnel, Public Grievances & Pensions, "Right to Privacy Bill, 2011," Press Information Bureau, Government of India, 18 August 2011, available at: https://pib.gov.in/newsite/erelcontent.aspx?relid=74743.

[6] Elonnai Hickok, "Report of the Group of Experts on Privacy vs. The Leaked 2014 Privacy Bill," The Centre for Internet and Society, 14 April 2014, available at: https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy-vs-leaked-2014-privacy-bill.

[7] Planning Commission, "Report of the 'Group of Experts on Privacy'" (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court) 16 October 2012, available at: https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf.

[8] "Justice Krishna to Head Expert Group on Data Protection Framework for India," Press Information Bureau, Government of India, 01 August 2017, available at: https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420.

[9] Seema Chishti, "Eminent Citizens Write to the Committee of Experts on Data Protection Framework," (The Indian Express, 06 November 2017), available at: https://indianexpress.com/article/india/citizens-group-questions-data-privacy-panel-composition-aadhaar-4924220/.

[10] "Draft Personal Data Protection Bill, 2018," PRS Legislative Research, accessed February 2, 2023, https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018 ["**Justice Srikrishna Committee Report**".

[11] Lok Sabha Debate of 11 December 2019, Seventeenth Series, Vol. VI, Second Session, 2019/1941, available at: https://sansad.in/getFile/debatestextmk/17/II/11.12.2019m.pdf?source=loksabhadocs

[12] Lok Sabha, "Joint Committee on the Personal Data Protection Bill, 2019", 16 December 2021, available at: https://eparlib.sansad.in/handle/123456789/835465?view_type=search ["**JPC Report**"].

[13] Lok Sabha Debate of 03 August 2022, Seventeenth Series, Vol. XX, Ninth Session, 2022/194 available at: https://sansad.in/getFile/debatestextmk/17/IX/03.08.2022.pdf?source=loksabhadocs, 894.

received comments on the Bill till an extended date of 02 January 2023.[14] The notice that came along with the DPDPB, 2022, stated that the submissions will not be disclosed to the public, because it will be held in a "fiduciary" capacity to enable persons submitting feedback to provide the same freely.

The MeitY received the comments and revised the Bill, but it left many concerns unaddressed. These concerns included wide exemptions granted to government instrumentalities that may facilitate increased state surveillance, amendment of the Right to Information Act, 2005 ("**RTI Act**") exempting any information that contains personal data from disclosure, level of executive control over the Data Protection Board, and the imposition of duties and penalties on Data Principals. On 31 January 2023, the Solicitor General stated before the Supreme Court of India that "a Data Protection Bill, after administrative compliances, is to be introduced before the Parliament in the second half of the Budget Session, 2023".[15] On 07 August 2023, the Digital Personal Data Protection Bill, 2023 ("**DPDPB, 2023**") was introduced in the Lok Sabha, discussed for a total of 52 minutes with 9 members participating in the debate, and passed on the same day amidst much protest.[16] The DPDPB, 2023, was introduced in the Rajya Sabha on 09 August 2023, the legislation was passed after 1 hour 7 minutes of debate with 7 Members speaking on the bill.[17] On 05 January 2025, the MeitY published the draft Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") inviting comments from the public till 05 March 2025.[18] The MeitY refused to share a copy of the comments received on the DPDP Rules by citing Section 8(1)(e) of the RTI Act which

---

[14] MeitY, The draft Digital Personal Data Protection Bill, 2022, Notice, and explanatory note, 18 November 2022, available at: https://drive.google.com/drive/folders/1KwMY7uCfZJtpa2GeR4xhMOkcrmUZjtQ4?usp=share_link; PIB, MeitY invites feedback on the draft 'Digital Personal Data Protection Bill 2022', 18 November 2022, available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1877030; The Hindu Bureau, Deadline for comments on digital data protection Bill extended, (The Hindu, 17 December 2022), available at: https://www.thehindu.com/news/national/deadline-for-comments-on-digital-data-protection-bill-extended/article66274776.ece; Anushka Jain, Read our public brief on the draft Digital Personal Data Protection Bill, 2022, (Internet Freedom Foundation, 16 February 2023), available at: https://internetfreedom.in/read-our-public-brief-on-the-draft-digital-personal-data-protection-bill-2022/.

[15] Sohini Chowdhury, "Data Protection Bill To Be Introduced In Parliament In Budget Session : Centre Tells Supreme Court," (LiveLaw, 31 January 2023), available at: https://www.livelaw.in/top-stories/data-protection-bill-to-be-introduced-in-parliament-in-budget-session-centre-tells-supreme-court-220372.

[16] MeitY, The draft Digital Personal Data Protection Bill, 2023 (all versions from the Parliament), available at: https://drive.google.com/drive/folders/1GQCaQt3VhWKgxE8UiKJfxP2Iu6n3XbUa?usp=share_link; Sansad TV, Minister Ashwini Vaishnaw introduces The Digital Personal Data Protection Bill, 2023, https://youtu.be/PyX4ckqcuDM?si=3sKHVCdRYFN8YdaF; IFF, On Parliament, 7 August 2023, available at: https://x.com/IFFonParliament/status/1688470057972563969?s=20.

[17] Sansad TV, Voting & Passing of The Digital Personal Data Protection Bill, 2023, available at: https://youtu.be/bXpQDggJcA8?si=cO1qCR-G3FM85rAx; IFF, On Parliament, 9 August 2023, available at: https://x.com/IFFonParliament/status/1689236700113879041?s=20.

[18] MeitY, draft Digital Personal Data Protection Rules, 2025, available at: https://innovateindia.mygov.in/dpdp-rules-2025/; Karthika Rajmohan & Ors., First Read on the Digital Personal Data Protection Rules 2025: Here's what you need to know, (Internet Freedom Foundation, 9 January 2025), available at: https://internetfreedom.in/first-read-on-the-dpdp-rules-2025/

exempts information held in a fiduciary capacity.[19] On 13 November 2025, the DPDP Rules were published in the gazette.

3. Private member Bills

There have been six notable efforts to introduce various models of privacy protection by honourable members of the Lok and Rajya Sabha. These are listed in a tabular form below.

House and date	Short title	Member	Status
Rajya Sabha on 28/11/2014	The Personal Data Protection Bill, 2014	V.J. Darda	Lapsed
Rajya Sabha on 05/08/2016	Right to Privacy of Personal Data Bill, 2016	Vivek Gupta	Lapsed
Lok Sabha on 10/03/2017	Right to Privacy of Personal Data Bill, 2016	Om Prakash Yadav	Lapsed
Lok Sabha on 21/07/2017	Data (Privacy and Protection) Bill, 2017	Baijayant Panda	Lapsed
Lok Sabha on 03/08/2018	Data Privacy and Protection Bill, 2017	Shashi Tharoor	Lapsed
Lok Sabha on 26/07/2019	Personal Data and Information Privacy Code Bill, 2019	D. Ravikumar	Lapsed

4. Right to Privacy Judgment

On 24 August 2017, the Supreme Court, in the case of *Justice KS Puttaswamy v. Union of India (I), (2017) 10 SCC 1, (*"**K.S. Puttaswamy (I)**"*)*, reaffirmed "privacy" as a fundamental right under Part III of the Constitution of India.[20] It directed the Government to bring out a robust data protection regime having due regard to *K.S. Puttaswamy (I)*.[21] The judgment noted that any law which encroaches upon the right to privacy must fulfill the three-fold requirement of (i) legality or the existence of law; (ii) a need, defined in terms of a legitimate State aim; and (iii) proportionality which ensures a rational nexus between the objects and the means

[19] MeitY's response to RTI Registration No. DITEC/R/E/25/00395, dated 17 April 2025, available at: https://drive.google.com/file/d/1M40fDN5JNZFgvJLzscMsPlwMp72nb6-5/view?usp=sharing.
[20] K.S. Puttaswamy v. Union of India (I), (2017) 10 SCC 1 ["K.S. Puttaswamy (I)"].
[21] K.S. Puttaswamy, [328], "*...Since the Union Government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union Government having due regard to what has been set out in this judgment*".

adopted to achieve them, and absence of less restrictive measures to achieve the aim.[22] In the context of Article 21 of the Constitution of India, any invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable.[23]

II. SCOPE OF THE DPDP ACT

The scope of India's new data protection law extends to both processing of digital and non-digital personal data that is subsequently digitized.[24] The DPDP Act does not cover personal data available in physical records, which is a narrower scope from the European Union's General Data Protection Framework ("**GDPR**").[25] The personal data must be processed within the territory of India, or, must have a connection with any activity related to offering of goods or services to Data Principals within the territory of India.[26]

The data protection law does not apply to personal data processed by an individual for:[27]

a. any personal or domestic purpose; or
b. personal data that is made or caused to be made publicly available by the person to whom the data relates (Data Principal) or any other person who is under an obligation under any law to make such data publicly available.

The scope of the DPDP Act, like the GDPR,[28] does not apply to individuals processing personal data for any personal or domestic purpose. Drawing a parallel with Singapore's Personal Data Protection Act of 2012,[29] the DPDP Act introduces a broad exemption for personal data that has been publicly disclosed. The DPDP Act illustrates this by noting that the DPDP Act will not apply to the personal data of an individual that has been made available on social media willingly by such individual while blogging. This will potentially exempt the use of personal data available online for AI training, given that such data is often willingly shared by individuals on social media.

III. A GUIDE TO THE CONSENT FRAMEWORK UNDER THE DPDP ACT

This section explains the defined persons in the DPDP Act, namely, Data Principals, Data Fiduciaries, and Consent Managers. It also considers the grounds for processing personal data,

[22] K.S. Puttaswamy, [325].
[23] K.S. Puttaswamy, [325].
[24] DPDP Act, s. 3(a).
[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> ["**GDPR**"].
[26] DPDP Act, s. 3(b).
[27] DPDP Act, s.3(c).
[28] GDPR, recital (18), Art 2(2)(c).
[29] Personal Data Protection Act of 2012 [SG], Clause 1 of Part II of First Schedule, "*[t]he collection, use or disclosure (as the case may be) of personal data about an individual that is publicly available*".

notice and consent regime in the DPDP Act, and legitimate uses that do not have to obtain consent from the Data Principal for processing personal data. Lastly, this section also considers processing of personal data belonging to children and persons with disabilities under the DPPD Act.

1. DEFINED PERSONS

Data Principals

Data Principal - s. 2(j)

Individuals (i.e. ordinary users) to whom the personal data relates. If the personal data belongs to a child or a person with disability, it includes their lawful guardian acting on their behalf.

Examples of Data Principal

- User of social media
- User of websites or apps of a bank
- Students, teachers, and professors of educational institutions
- Patient registered with a hospital
- Voters whose details are available on the Election Commission of India

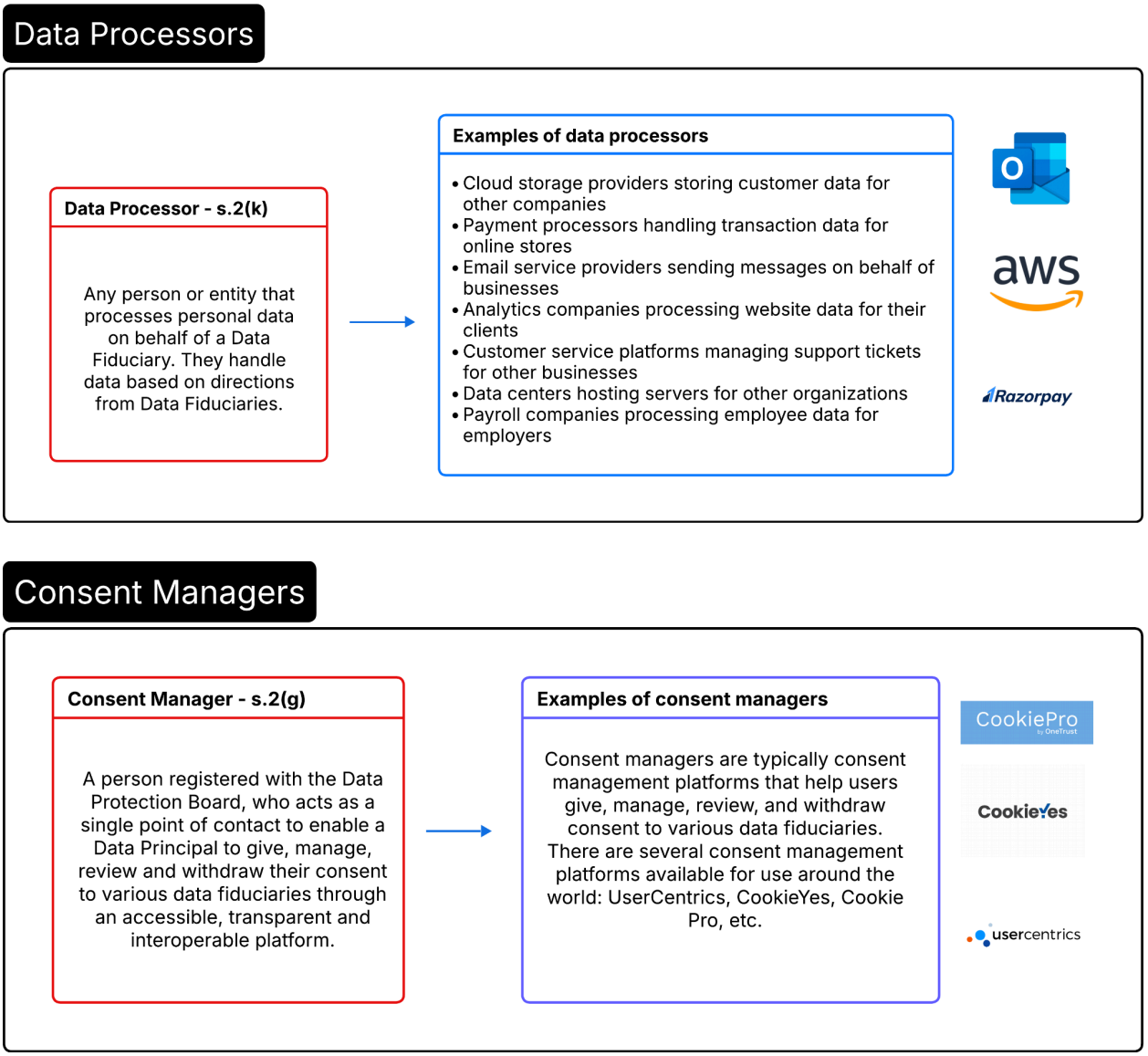
Data Fiduciaries

Data Fiduciary - s.2(i)

Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. They determine what data to collect from users and what to do with it.

Examples of data fiduciaries

- E-commerce companies deciding what customer information to collect for orders and shipping
- Social media platforms choosing what user data to gather for their services
- Healthcare providers determining what patient information they need to deliver care
- Banks selecting what financial data to collect for account management
- Educational institutions deciding what student information to maintain
- Mobile app developers choosing what user data their app will collect



2. PROCESSING OF PERSONAL DATA

2.1. Grounds for processing personal data

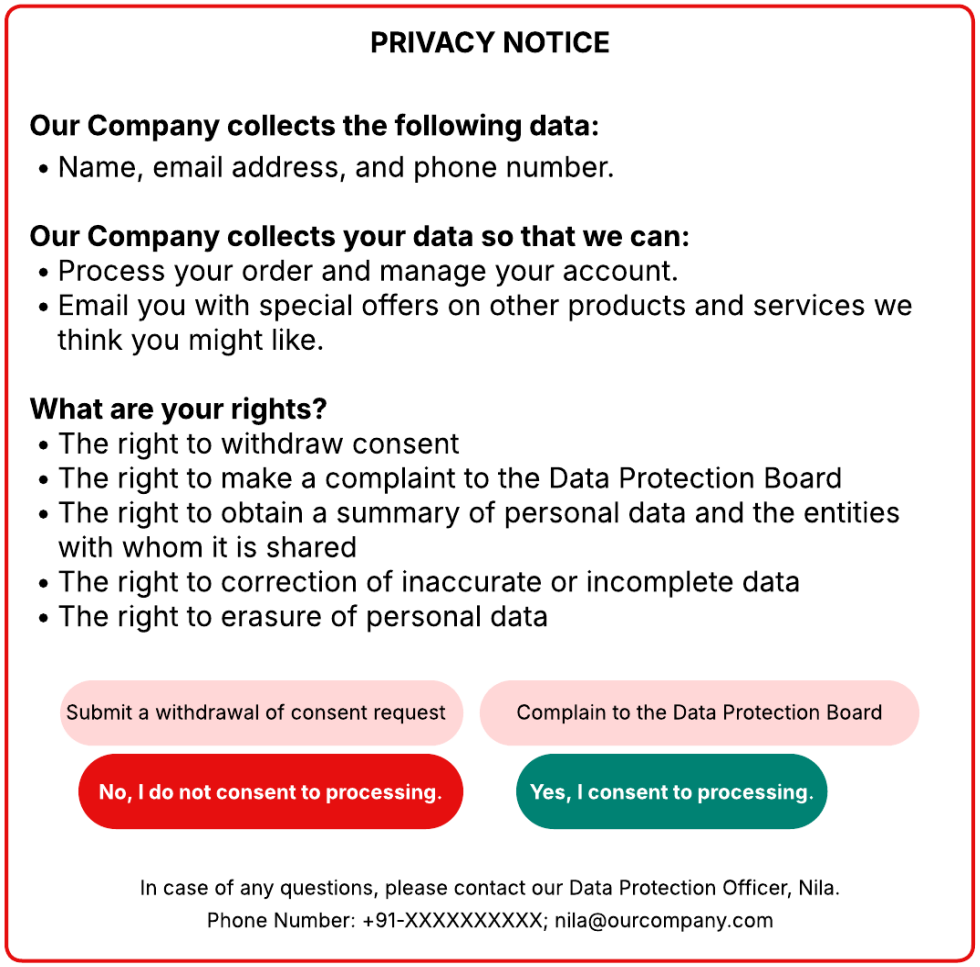
Section 4 of the DPDP Act states that a person may process the personal data of a Data Principal only in accordance with the provisions of the Act and for purposes not expressly forbidden by any other law.

There are two grounds for processing personal data, namely—

- **Processing personal data upon consent from Data Principal**: In the first ground for processing of personal data, the Data Fiduciary gives notice to the Data Principal prior to using or processing personal data, to which the Data Principal can give or deny consent. This notice and consent regime is further explained below in Section B.2.

- **Processing personal data for "certain legitimate uses" even without the consent of the Data Principal:** In the second ground for processing personal data, a Data Fiduciary may process personal data of a Data Principal for "certain legitimate uses" even without the consent of the Data Principal. This vests large amounts of discretion on Data Fiduciaries to process personal data even when the Data Principal has not provided consent. The "legitimate uses" ground can be used to circumvent the more onerous notice and consent regime. The "legitimate uses" are further explained below in Section B.3.

2.2. Notice and Consent Regime



2.2.1. Notice given by Data Fiduciary

Every Data Fiduciary must place a request in the form of a notice to the Data Principal for use or processing of personal data.[30] This notice must be understandable independently of any other information, in clear and plain language, such that the Data Principal can give specific and

[30] DPDP Act, s. 5(1).

informed consent for the processing of their personal data.[31] The notice must contain the following details:[32]

i. The personal data and the intended purpose (specific description of the goods or services to be provided by such processing) for which the same is proposed to be processed;
ii. The manner in which the Data Principal may withdraw her consent under section 6(4) or redress grievances under section 13 of the DPDP Act;
iii. The manner in which the Data Principal may exercise their rights under the DPDP Act;
iv. The manner in which the Data Principal may make a complaint to the Data Protection Board;
v. Contact information of a Data Protection Office or any other person who is able to answer questions about processing of personal data on behalf of the Data Fiduciary.

In case of Data Fiduciaries who are already processing personal data of Data Principals after having obtained their consent previously, such Data Fiduciaries are required to seek renewed consent in accordance with the notice requirements outlined above.[33] The Data Fiduciary is permitted to process the personal data until the Data Principal actively withdraws her prior consent.[34] The Data Principal must have the option of viewing the notice in English or any of the languages specified in Eighth Schedule of the Indian Constitution.[35]

2.2.2. Consent given by Data Principal

Definition of consent: Consent given by a Data Principal should 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.[36] In practice, this may mean that data fiduciaries cannot rely on "bundled consent". The absence of a valid consent constitutes an infringement of the provisions of the DPDP Act and rules.[37] To this extent, an illustration to Section 6(2) of the DPDP Act specifically states that consenting to waiving off the right to file a complaint to the Data Protection Board is invalid.

Proof of consent: If the question of validity of consent arises in a court of law, it is on the Data Fiduciary to prove that a notice was given by her to the Data Principal and consent was given by

[31] DPDP Rules, rule 3(a)-3(b).
[32] DPDP Act, s. 5(1); DPDP Rules, rule 3(b), 9.
[33] DPDP Act, s. 5(2)(a).
[34] DPDP Act, s. 5(2)(b).
[35] DPDP Act, s. 5(3).
[36] DPDP Act, s. 6(1).
[37] DPDP Act, s. 6(2).

such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.[38]

The right to withdraw consent: The Data Principal has the right to withdraw her consent to processing of her personal data at any time.[39] The withdrawal process must be as easy as the process for consent, and should not be made unnecessarily cumbersome. Any consequences of the withdrawal are to be borne by the Data Principal.[40] Withdrawal of consent at any time does not affect the legality of processing that occurred prior to withdrawal.

2.3. Consent Manager

2.3.1. Role of Consent Manager

Consent Managers are persons registered with the Data Protection Board, who act as a single point of contact to enable the Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform.[41]

Such persons or entities must have fulfilled technical, operational, financial and other conditions.[42] These conditions include:[43]

i) An applicant for Consent Manager is a company incorporated in India.
ii) The financial condition of the company and the general character of its management must be sound. Volume of business and earning potential must be adequate.
iii) Net worth must be not less than two crore rupees.
iv) Key management personnel should be individuals with a general reputation and record of fairness and integrity.
v) The operations proposed to be undertaken by the applicant are in the interests of Data Principals.
vi) The memorandum of association and articles of association of the applicant company should state that the company adheres to obligations concerning conflict of interest in Part B of First Schedule to DPDP Rules. These provisions can only be amended with board approval.
vii) Consent Management companies must be independently certified that they have:

    i. an interoperable platform to give, manage, review and withdraw her consent is consistent with such data protection standards and assurance framework; and

[38] DPDP Act, s.6(10).
[39] DPDP Act, s. 6(4).
[40] DPDP Act, s. 6(5).
[41] DPDP Act, s. 2(g).
[42] DPDP Act, s. 6(9); DPDP Rules, rules 4(1), 4(2), Part A of First Schedule.
[43] DPDP Rules, rules 4(1), 4(2), Part A of First Schedule.

ii. appropriate technical and organizational measures are in place to ensure adherence to such standards and framework, including the effective observance of the obligations under item 11 of Part B of First Schedule to DPDP Rules requiring key information to be published on website and app.

2.3.2. Obligations of Consent Manager

The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.[44] The Consent Manager shall be accountable to the Data Principal. The obligations specified in the DPDP Rules for consent managers include:[45]

i) The Consent Manager acts in a *fiduciary capacity* in relation to the Data Principal.

ii) The Consent Manager shall enable a Data Principal using its platform (website/app or both) to give consent to a Data Fiduciary, either directly or indirectly.
   a. **Direct consent:** When a bank sends a request via a consent management platform to X to process her personal data available in her bank account statement, X can use the same platform to directly give consent to the bank and give access to her bank account statement as a digital record.
   b. **Indirect consent:** Bank 1 sends a request to X via a consent management platform for processing personal data contained in her bank statement with Bank 2. X can use the consent management platform to route her consent through Bank 2 to Bank 1, while also digitally instructing Bank 2 to send her bank account statement to Bank 1. Bank 2 proceeds to send the bank account statement to Bank 1.

iii) No personal data on the Consent Manager's platform shall be readable by such Consent Manager. This would require that all personal data is anonymized or pseudonymized.

iv) Consent Manager shall maintain a record of the following information on its platform:

   a. Consents given, denied or withdrawn by the Data Principal;
   b. Notices or requests for consent; and
   c. Sharing of her personal data with a transferee Data Fiduciary.

v) The Consent Manager shall share the record maintained by it to the Data Principal. It shall also provide the information in machine-readable form if required. The record

[44] DPDP Act, s. 6(7).
[45] DPDP Rules, Part B of First Schedule.

must be maintained for at least seven years, or for such a longer period as agreed between the Data Principal and Consent Manager, or as may be required by law.

vi) The Consent Manager shall not sub-contract or assign the performance of any of its obligations under the DPDP Act and the DPDP Rules.

vii) The Consent Manager shall take reasonable security safeguards to prevent personal data breach.

viii) **Conflict of interest:** The Consent Manager shall avoid conflict of interest with Data Fiduciaries, including in respect of their promoters and key managerial personnel. The Consent Manager must ensure that no conflict of interest arises on account of directors, key managerial personnel and senior management holding a directorship, financial interest, employment or beneficial ownership in Data Fiduciaries, or having a material pecuniary relationship with them.

ix) The Consent Manager's website and app shall have information regarding:

a. the promoters, directors, key managerial personnel and senior management of the Consent Manager company;
b. every person who holds shares in excess of 2% of the shareholding of the Consent Manager company;
c. every body-corporate in which, any promoter, director, key managerial personnel or senior management of the Consent Manager, holds shares in excess of 2% as on the first day of the preceding calendar month;
d. such other information as the Board may direct the Consent Manager to disclose in the interests of transparency.

x) The Consent Manager shall have effective audit mechanisms to review, monitor, evaluate and report to the Board periodically or on directions of the Board, on: technical and organizational controls, systems, procedures and safeguards; continued fulfilment of registration conditions, and adherence to obligations under the DPDP Act and DPDP Rules.

xi) The control of the Consent Manager company shall not be transferred by way of sale, merger or otherwise, except with the previous approval of the Data Protection Board and subject to fulfilment of such conditions as the Board may specify.

2.3.3. Non-adherence to obligations of Consent Managers

If the Data Protection Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations, it may, after giving an opportunity of being heard, inform the Consent

Manager of such non-adherence and direct the Consent Manager to take measures to ensure adherence.[46]

2.3.4. Actions to protect Data Principal's interest

If the Data Protection Board is satisfied that the interests of the Data Principal ought to be protected, the Data Protection Board may, after giving the Consent Manager an opportunity of being heard, and after recording the reasons in writing—

a. suspend or cancel the registration of such Consent Manager; and
b. give such directions as it may deem fit to that Consent Manager.

2.3.5. Call for information

The Data Protection Board may require the Consent Manager to furnish such information as required.[47]

2.3.6. 'Legitimate Uses' that do not require consent

As explained earlier, a Data Fiduciary may process personal data of a Data Principal for "certain legitimate uses" even without the consent of the Data Principal. The "legitimate uses" ground can be used to circumvent the more onerous notice and consent regime.

2.3.7. Where the Data Principal has voluntarily provided personal data to the Data Fiduciary, without explicitly denying consent to the Data Fiduciary for use of her personal data[48]

This carveout from the consent regime is ripe for abuse. For example, one of the illustrations provided under Section 7(a) is an individual who makes a purchase at a pharmacy and where she "voluntarily" provides her personal data and requests the pharmacy to acknowledge payment by sending receipt via messages. The pharmacy will process the phone number through their billing system of the individual to send her the receipt. However, instances of people not being able to make a purchase or obtain a service without providing phone numbers are not unknown, and this carveout from the consent regime is overbroad and could effectively operate as a disproportionate intrusion into the privacy of individuals. Another example would be when a person voluntarily provides their name and Aadhar number for checking ration card status to a person or civil society

[46] DPDP Rules, rule 4(4).
[47] DPDP Rules, rule 4(6).
[48] DPDP Act, s. 7(a).

organization, and does not explicitly deny consent for processing, the notice and consent regime does not apply.

2.3.8. Use by State and any of its instrumentalities, for one of the following purposes

The DPDP Act specifies two instances when the State and any of its instrumentalities can process personal data without the consent of the Data Principal.

First, the State and any of its instrumentalities can process personal data without the consent of the Data Principal to provide or issue any subsidy, benefit, service, certificate, license, or permit to the Data Principal.[49] This carveout is applicable to persons who have previously consented to processing of personal data for any subsidy, benefit, license etc., or if such personal data is available in digital/physical form and digitised subsequently, from any other register or database which is maintained by the State or its instrumentalities. This carveout is applicable if such subsidy, benefit, service, certificate, licence or permit was provided:

a. on account of any State function or the function of any of the State's instrumentalities under any law for the time being in force;
b. under any policy or instruction issued by the Central Government or a State Government in exercise of its executive power; and
c. using public funds by incurring expenditure on the same from, or with accrual of receipts to, —
    i. **in case of the Central Government**: Consolidated Fund of India or public account of India;
    ii. **in case of a State Government:** Consolidated Fund of the State or public account of the State; or
    iii. **in case of any local or other authority within the territory of India or under the control of the Government of India or of any State:** the fund or funds of such authority.

Processing of any personal data by the State and its instrumentalities under this ground should be in accordance with the policy or standards issued by the Central Government for governance of personal data.[50] The standards for processing personal data are that processing must be carried out in a lawful manner, and for the uses specified in section 7(b) of the DPDP Act. Processing can be done while making reasonable efforts to ensure the completeness, accuracy and consistency of personal data. Reasonable security safeguards must be put in place to prevent personal data breach. Where processing is to be done, the Data Principal must be:

[49] DPDP Act, s. 7(b).
[50] DPDP Act, s. 7(c); DPDP Rules, rule 5(1); Second Schedule to DPDP Rules specify standards to be followed.

a. intimated with the business contact information of the Data Protection Officer or such other officer who can answer questions about the processing of personal data;
b. sent particular links for accessing the website/app of the Data Fiduciary and a description of accessing others rights that the Data Principal has under the DPDP Act;
c. carried on in a manner consistent with other standards applicable to processing of personal data under policy issued by the Central Government or any law for the time being in force; and
d. accountability of the person who alone or in conjunction with other persons determines the purpose and means of processing of personal data, for effective observance of these standards.

Two, the State and any of its instrumentalities can process personal data without the consent of the Data Principal to perform any function under any law for the time being in force in India, or in the interest of sovereignty and integrity of India, or security of the State. Whereas under this provision, the State and instrumentalities are *permitted* to process data without consent; under Section 17(2)(a), notified instrumentalities are *exempted* from the requirements of the DPDP Act entirely. Given that both these provisions operate outside the notice and consent regime, Data Principals will have no control over the use and processing of their personal data.

2.3.9. Use by any person to fulfill a legal obligation or comply with a court order

Any person who needs to process personal data for 'fulfilling any obligation under any law' for the time being in force in India, that may require disclosure of any information to the State or any of its instrumentalities can do so without seeking consent of the Data Principal.[51]

Likewise, the consent of the Data Principal need not be sought in respect of personal data that needs to be processed for:[52]

a. complying with any judgment or decree or order issued under any law for the time being in force in India; or
b. any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India.

2.3.10. For responding to medical emergencies, epidemics, and disasters

Consent of the Data Principal is not required to process personal data:

a. 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;[53]

[51] DPDP Act, s. 7(d).
[52] DPDP Act, s. 7(e).
[53] DPDP Act, s. 7(f).

b. 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;[54]
c. For taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.[55]

2.3.11. For the purposes of employment or those related to safeguarding the employer from loss or liability[56]

The employer is permitted to process personal data to prevent corporate espionage, maintain confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee. Under this provision, certain measures that are strictly within the terms of this clause such as end point protection, logging, device monitoring, etc. could be justified as intended to prevent corporate espionage or confidential information leakages. Similarly, other purpose-based necessities in offices that are sought out by employees such as employee meals or creche facilities would require processing personal data. However, certain other processing of personal data could also be read as being impliedly permitted "for the purpose of employment". This includes mandatory payroll processing, processing for tracking leave, providing statutory employment benefits, or carrying out actions mandated for employers under law. This allows employers to circumvent the notice and consent regime, falling back on the "legitimate uses" basis to abuse the DPDP Act.

IV. CONSENT PROCESS FOR CHILDREN OR PERSONS WITH DISABILITY

Data Fiduciaries must seek "verifiable consent" of the parent of a child or lawful guardian, as the case may be, prior to processing any personal data of a child or a person with disability.[57]

1. Verifiable consent in the case of children

The DPDP Act states that a Data Fiduciary shall obtain verifiable consent of a parent to process personal data of a child.[58] It also states that Data fiduciaries shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.[59]

Verifiable consent can be obtained by referring to:[60]

a. Reliable details of identity and age of the individual available with the Data Fiduciary;
b. Details of identity and age voluntarily provided:
    i. by the individual on their own, or

[54] DPDP Act, s. 7(g).
[55] DPDP Act, s. 7(h).
[56] DPDP Act, s. 7(i).
[57] DPDP Act, s. 9(1).
[58] DPDP Act, s.9(1); DPDP Rules, rule 10(1).
[59] DPDP Act, s. 9(3).
[60] DPDP Rules, rule 10(1).

ii. through a virtual token mapped to details issued by an authorised entity.

An authorised entity is an entity entrusted by law, by the Central Government, or by the State Government with the issuance of details of the identity and age or a virtual token mapped to such details.[61] It can also be a person appointed or permitted by such an authorised entity who can access the identity and age details provided by way of a Digital Locker service provider. Digital Locker service providers are intermediaries notified by the Central Government in accordance with rules under the Information Technology Act, 2000.[62]

Processing children's personal data is prohibited when it is likely to cause any detrimental effect on the well-being of a child.[63]

2. Exemption from verifiable consent and restrictions on tracking or behavioral monitoring

The requirement on "verifiable consent" and restrictions on tracking or behavioral monitoring,[64] are not applicable to processing of personal data of a child by:[65]

a. certain classes of notified data fiduciaries that are verifiably safe (such as clinical establishments, child day care centers, and educational institutions); or
b. when the processing is intended for such purposes (such as for determining real time location of a child, information detrimental to children is not accessible by them).

The classes of data fiduciaries and the conditions under which they are exempted from the requirements of "verifiable consent" and restrictions on tracking or behavioral monitoring are as follows:[66]

FOURTH SCHEDULE

[*See* rule 12]

PART A

Classes of Data Fiduciaries in respect of whom provisions of sub-sections (1) and (3) of section 9 shall not apply

S. No.	Class of Data Fiduciaries	Conditions
(1)	(2)	(3)
1.	A Data Fiduciary who is a clinical establishment, mental health establishment or healthcare professional.	Processing is restricted to provision of health services to the child by such establishment or professional, to the extent necessary for the protection of her health.
2.	A Data Fiduciary who is an allied healthcare professional.	Processing is restricted to supporting implementation of any healthcare treatment and referral plan

[61] DPDP Rules, rule 10(2)(b).
[62] DPDP Rules, rule 10(2)(c).
[63] DPDP Act, s. 9(2).
[64] DPDP Act, s. 9(1), 9(3).
[65] DPDP Act, s. 9(4); DPDP Rules, rule 12.
[66] DPDP Rules, Part A of Fourth Schedule.

		recommended by such professional for the child, to the extent necessary for the protection of her health.
3.	A Data Fiduciary who is an educational institution.	Processing is restricted to tracking and behavioural monitoring— (a) for the educational activities of such institution; or (b) in the interests of safety of children enrolled with such institution.
4.	A Data Fiduciary who is an individual in whose care infants and children in a crèche or child day care centre are entrusted.	Processing is restricted to tracking and behavioural monitoring in the interests of safety of children entrusted in the care of such institution, crèche or centre.
5.	A Data Fiduciary who is engaged by an educational institution, crèche or child care centre for transport of children enrolled with such institution, crèche or centre.	Processing is restricted to tracking the location of such children, in the interests of their safety, during the course of their travel to and from such institution, crèche or centre.

The purposes which are exempted from the requirements of "verifiable consent" and restrictions on tracking or behavioral monitoring, and the conditions under which such exemption is applicable, is as follows:[67]

PART B

Purposes for which provisions of sub-sections (1) and (3) of section 9 shall not apply

S. No.	Purposes	Conditions
(1)	(2)	(3)
1.	For the exercise of any power, performance of any function or discharge of any duties in the interests of a child, under any law for the time being in force in India.	Processing is restricted to the extent necessary for such exercise, performance or discharge.
2.	For providing or issuing of any subsidy, benefit, service, certificate, licence or permit, by whatever name called, under law or policy or using public funds, in the interests of a child, under clause (b) of section 7 of the Act.	Processing is restricted to the extent necessary for such provision or issuance.
3.	For the creation of a user account for communicating by email.	Processing is restricted to the extent necessary for creating such user account, the use of which is limited to communication by email.
4.	For the determination of real-time location of a child.	Processing is restricted to the tracking of real-time location of such child, in the interest of her safety and protection or security.
5.	For ensuring that any information, service or advertisement likely to cause any detrimental effect on the well-being of a child is not accessible to her.	Processing is restricted to the extent necessary to ensure that such information, service or advertisement is not accessible to the child.
6.	For confirmation by the Data Fiduciary that the Data Principal is not a child and observance of due diligence under rule 10.	Processing is restricted to the extent necessary for such confirmation or observance.

[67] DPDP Rules, Part B of Fourth Schedule.

3. Verifiable consent in the case of persons with disabilities

A Data Fiduciary shall observe due diligence to verify that the lawful guardian of a person with disability, is a guardian appointed by a court of law, or by a designated authority,[68] or by a local level committee,[69] under the law applicable to guardianship.[70]

The rules state that the "law applicable to guardianship" is as follows:

- **Rights of Persons with Disabilities Act, 2016:** in the case of an individual who has "long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who despite being provided adequate and appropriate support is unable to take legally binding decisions".[71]
- **National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999:** in the case of "a person who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of such conditions and includes a person suffering from severe multiple disability".[72]

V. CORE OBLIGATIONS OF DATA FIDUCIARIES

1. General Obligations of the Data Fiduciary

Section 8 of the DPDP Act lists the general obligations that the Data Fiduciaries are bound by. These obligations are as follows:

1.1. Securing Compliance with the law

A Data Fiduciary shall be responsible for securing compliance with the provisions of the DPDP Act and DPDP Rules concerning any processing that is carried out by the Data Fiduciary itself or on behalf of the Data Fiduciary by a Data Processor.[73] The Data Fiduciary is obligated to undertake such compliance *irrespective* of any agreement to the contrary or a failure of the Data Principal to carry out its duties (as provided under Section 15 of the DPDP Act).

---

[68] Designated authority will be an authority designated under section 15 of the Rights of Persons with Disabilities Act, 2016 (49 of 2016) to support persons with disabilities in exercise of their legal capacity. For e.g. the District Collector is specified as the Designated Authority under the Tamil Nadu Rights of Persons with Disabilities Rules, 2018.

[69] The local level committee constituted under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999.

[70] DPDP Rules, rule 11(1).

[71] DPDP Rules, rule 11(2)(b)(i).

[72] DPDP Rules, rule 11(2)(b)(ii).

[73] DPDP Act, s. 8(1).

1.2. Engaging a Data Processor under a Valid Contract

A valid contract between the Data Fiduciary and the Data Processor is mandated in order for a Data Fiduciary to engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals.[74]

1.3. Ensuring the Data's Completeness, Accuracy and Consistency

A Data Fiduciary processing personal data is obligated to ensure the data's completeness, accuracy and consistency where such data is likely to be used to make a decision that affects the Data Principal or is likely to be disclosed to another Data Fiduciary.[75]

1.4. Implementing technical and organisational measures

A Data Fiduciary is obligated to implement appropriate technical and organisational measures to ensure that the DPDP Act and DPDP Rules are observed in an effective manner.[76]

1.5. Taking Reasonable Security Safeguards

A Data Fiduciary is obligated to take "reasonable security safeguards" to prevent a personal data breach and protect the personal data that is in its possession or under its control.[77] This includes any processing of such personal data that is carried out by the Data Fiduciary or by a Data Processor, on behalf of the Data Fiduciary.

The minimum measures that constitute taking "reasonable security safeguards" that a Data Fiduciary is obligated to take, are as follows:[78]

a. take appropriate data security measures, such as securing of personal data through encryption, obfuscation, masking or the use of virtual tokens mapped to that personal data;
b. take appropriate measures, wherever applicable, to control access to the computer resources used by the Data Fiduciary or the Data Processor;
c. visibility on the accessing of such personal data (through appropriate logs), monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;
d. take reasonable measures (for instance through data-backups) for continued processing in the event of confidentiality, integrity or availability of the personal data being compromised due to destruction or loss of access to it or otherwise;

[74] DPDP Act, s. 8(2).
[75] DPDP Act, s. 8(3).
[76] DPDP Act, s. 8(4).
[77] DPDP Act, s. 8(5).
[78] DPDP Rules, rule 6.

e. for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of a compromise;
f. to retain such logs and personal data for a period of one year;
g. to provide for taking reasonable security safeguards in the contract entered into between the Data Fiduciary and the Data Processor; and
h. take appropriate technical and organisational measures to ensure effective observance of security safeguards.

1.6. Intimation upon occurrence of Data Breach

In the event that a personal data breach takes place, the Data Fiduciary is obligated to intimate the Data Protection Board (DPB) and each Data Principal who is affected by such data breach, in the prescribed form and manner.[79] These obligations are as follows:

1.6.1. Obligation of the Data Fiduciary to Intimate the Data Principal about a Data Breach

The DPDP Rules lay down the procedure to be followed by the Data Fiduciary regarding its obligation to intimate each affected Data Principal about the occurrence of a data breach.[80] On becoming aware of any personal data breach, the Data Fiduciary is obligated to intimate to each affected Data Principal, in a *concise, clear and plain manner* and without delay, about such data breach, to the best of the Data Fiduciary's knowledge. Such intimation to the Data Principal is to be carried out through their user account or any mode of communication registered by the Data Principal with the Data Fiduciary.

The intimation by the Data Fiduciary to the Data Principal about a data breach should comprise the following information:

- a description of the breach, including its nature, extent and the timing of its occurrence;
- the relevant consequences to the Data Principal, that are likely to arise from the breach;
- the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk;
- the safety measures that the Data Principal may take to protect their interests; and
- business contact information of a person who is able to respond to any queries of the Data Principal on the Data Fiduciary's behalf.

[79] DPDP Act, s. 8(6).
[80] DPDP Rules, rule 7(1).

1.6.2. Obligation of the Data Fiduciary to Intimate the Data Protection Board about a Data Breach

The Data Fiduciary is obligated to intimate the Data Protection Board (DPB) in the event of a personal data breach.[81] Further, such intimation to the Board must be done without delay, within a period of 72 hours of becoming aware of the breach (unless the period is allowed to be extended by the Board upon a written request)[82]. It must include a description of the breach, its nature, extent, timing and location of occurrence and the likely impact.

The Data Fiduciary is obligated to provide comprehensive information to the DPB.[83] The information provided to the DPB by the Data Fiduciary in this regard is as follows:

a. updated and detailed information regarding the breach's description (nature, extent, timing, location of occurrence, and impact of the breach);
b. the broad facts related to the events, circumstances and reasons leading to the breach;
c. measures implemented or proposed, if any, to mitigate risk;
d. any findings regarding the person who caused the breach;
e. remedial measures taken to prevent recurrence of such breach; and
f. a report regarding the intimations given to affected Data Principals.

1.7. Ensuring the Erasure of Personal Data upon Consent Withdrawal

A Data Fiduciary is obligated to erase the Data Principal's personal data upon the withdrawal of consent or as soon as it can be reasonably assumed that the "specified purpose" is no longer being served, whichever is earlier, unless the personal data's retention is necessary for compliance with any law.[84]

The "specified purpose" shall be deemed to not be served any longer, if the Data Principal does not approach the Data Fiduciary for the performance of the specified purpose. Further, if the Data Principal does not exercise any of their rights related to data processing for the prescribed time period then too, the purpose shall be deemed to not be served.

A Data Fiduciary who falls into a particular class and is processing personal data for such corresponding purposes (as set out in Third Schedule), is obligated to erase such personal data, unless its retention is required for compliance with any law or for the corresponding time period under the Third Schedule.[85] This is given that the Data Principal must neither have approached

[81] DPDP Rules, rule 7(2).
[82] DPDP Rules, rule 7(2)(b).
[83] DPDP Rules, rule 7(2)(b).
[84] DPDP Act, s. 8(7)(a).
[85] DPDP Rules, rule 8(1).

the Data Fiduciary for the performance of the specified purpose nor exercised their rights regarding the processing of the data.[86]

The Data Fiduciary shall inform the Data Principal that their personal data shall be erased upon completion of the prescribed period, at least 48 hours before completion of such period, unless the Data Principal logs into their user account/otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises their rights regarding the processing of the personal data.[87]

1.8. Timeline of retaining data as per Rule 8

A Data Fiduciary shall retain the personal data, associated traffic data and other logs of the processing for a *minimum period of one year* from the date of such processing, for the purposes specified under the Seventh Schedule, with respect of any processing of personal data undertaken by the Data Fiduciary or on its behalf by a Data Processor.[88]

After the completion of this period, the Data Fiduciary shall erase such personal data and logs, unless their further retention is required for compliance with any other law or the Data Fiduciary is notified to do so by the Government.[89]

THIRD SCHEDULE

[*See* rule 8(1)]

S. no.	Class of Data Fiduciaries	Purposes	Time period
(1)	(2)	(3)	(4)
1.	Data Fiduciary who is an e-commerce entity having not less than two crore registered users in India.	For all purposes, except for the following: (a) Enabling the Data Principal to access her user account; and (b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services.	Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest.
2.	Data Fiduciary who is an online gaming intermediary having not less than fifty lakh registered users in India.	For all purposes, except for the following: (a) Enabling the Data Principal to access her user account; and (b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data	Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest.

[86] ibid.
[87] DPDP Rules, rule 8(2).
[88] DPDP Rules, rule 8(3).
[89] ibid.

		Fiduciary, and may be used to get money, goods or services.	
3.	Data Fiduciary who is a social media intermediary having not less than two crore registered users in India.	For all purposes, except for the following: (a) Enabling the Data Principal to access her user account; and (b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services.	Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest.

The Data Fiduciary is further obligated to ensure that its Data Processor has erased any personal data that was provided to it by the Data Fiduciary for the purpose of processing.[90]

1.9. Publishing Contact Information of the Data Protection Officer

A Data Fiduciary is obligated to publish the business contact information of a Data Protection Officer (if applicable), or a person who is able to answer questions raised by the Data Principal about the processing of their personal data on the Data Fiduciary's behalf.[91]

Further, every Data Fiduciary shall prominently publish on its website or app, and mention in every response to a communication, the business contact information of the Data Protection Officer (if one is applicable).[92] Alternatively, the Data Fiduciary shall publish the business contact information of a person who is able to answer questions of the Data Principal about the processing of their personal data on behalf of the Data Fiduciary.

1.10. Establishing a Grievance Redressal Mechanism

A Data Fiduciary is obligated to establish an effective grievance redressal mechanism to address the grievances of Data Principals.[93]

2. Additional obligations of a Significant Data Fiduciary

A Significant Data Fiduciary ("**SDF**") refers to any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under Section 10(1) of the DPDP Act.[94] As per Section 10(1), the Central Government is empowered to notify any Data Fiduciary or class of

[90] DPDP Act, s. 8(7)(b).
[91] DPDP Act, s. 8(9).
[92] DPDP Rules, rule 9.
[93] DPDP Act, s. 8(10).
[94] DPDP Act, s. 2(z); 10(1).

Data Fiduciaries as a Significant Data Fiduciary, by evaluating relevant factors as it may determine, such as:

a. the volume and sensitivity of personal data processed;
b. risk to the rights of Data Principal;
c. potential impact on the sovereignty and integrity of India;
d. risk to electoral democracy;
e. security of the State; and
f. public order.

An SDF is tasked with certain additional obligations which are enumerated under Section 10(2) of the DPDP Act.[95] These obligations broadly include:

2.1 Appointment of a Data Protection Officer

A Significant Data Fiduciary is obligated to appoint a Data Protection Officer (DPO).[96] A DPO represents the SDF and must be based in India. The DPO is an individual responsible to the Board of Directors or a similar governing body of the SDF. The DPO is primarily responsible for being the point of contact for the grievance redressal mechanism under the DPDP Act.

2.2 Appointment of an independent Data Auditor

The SDF is obligated to appoint a Data Auditor who is independent, to carry out a data audit.[97] The Data Auditor shall be responsible for evaluating the SDF's compliance with the DPDP Act.

2.3 Other Measures

The SDF must undertake other measures, including a periodic Data Protection Impact Assessment, a periodic audit, and any other measures so prescribed under the DPDP Act.[98]

2.3.1. Conducting a Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment ("**DPIA**") is a process that generates a Report for the DPB's review, containing the following information:[99]

a. a description of the rights of Data Principals;
b. the purpose of processing of the Data Principal's personal data;

[95] DPDP Act, s.10(2).
[96] DPDP Act, s.10(2)(a).
[97] DPDP Act, s.10(2)(b).
[98] DPDP Act, s.10(2)(c).
[99] DPDP Act, s. 10(2)(c)(i).

c. an assessment of the risk to the Data Principals' rights;
d. management of the risk to the Data Principals rights; and
e. such other prescribed matters regarding the process.

A SDF shall carry out a DPIA and an audit to ensure effective observance of the DPDP Act and DPDP Rules once in every period of twelve (12) months from the date on which it is notified as a SDF.[100] Further, a SDF shall furnish the report from the person who carried out the DPIA and the audit containing their significant observations regarding each evaluation respectively.[101]

2.3.2. Technical Measures should not Pose a Risk to Data Principals

Other additional obligations by a SDF include measures such as observing due diligence to verify that technical measures that they have adopted are not likely to pose a risk to the rights of Data Principals.[102] These technical measures include algorithmic software adopted by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it.

2.3.3. Personal and Traffic Data not to be Transferred outside India

An SDF shall undertake measures to ensure that personal data specified by the Central Government (on the basis of the recommendations of a committee), is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.[103]

VI. CORE RIGHTS AND DUTIES OF DATA PRINCIPALS

1. The Rights of the Data Principal

Under the DPDP Act, the Data Principal is primarily entitled to four main rights. These are:

1. the right to access information about personal data;
2. the right to correction and erasure of personal data;
3. the right of grievance redressal; and
4. the right to nominate.

[100] DPDP Rules, rule 13(1).
[101] DPDP Rules, rule 13(2).
[102] DPDP Rules, Rule 13(3).
[103] DPDP Rules, Rule 13(4).

1.1. The Right to Access Information about Personal Data

The DPDP Act gives the Data Principal the right to obtain information about their personal data (to which they had previously accorded consent) on request being made to the Data Fiduciary in the prescribed manner.[104] This information includes:

a. a summary of personal data being processed by the Data Fiduciary;
b. the processing activities undertaken by the Data Fiduciary related to such personal data;
c. the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared;
d. a description of the personal data so shared by the Data Fiduciary; and
e. any other information related to the Data Principal's personal data and its processing, as prescribed.

Every Data Fiduciary shall publish on its app/website, the means of making the request and the particulars required by a Data Fiduciary such as username or identifier of the Data Principal to identify the user.[105] The Data Principal, to exercise their rights under the DPDP Act, may make a request to the Data Fiduciary through such means and using the username/identifier required by the Data Fiduciary. An "identifier" can be a set of characters that enable the identification of the Data Principal in the Data Fiduciary's user directory.[106] For example, an identifier could include, a customer identification file number, a customer acquisition form number, an application reference number, an enrolment ID, an email address, a mobile number or a licence number.[107]

1.1.1. DPDP Rules fail to specify timeline for processing Data Principals' requests

A major drawback of the DPDP Rules is that the framework under the Rules does not lay down a timeline for the processing and completion of requests to access personal data, which several data protection laws in other jurisdictions provide for in their respective frameworks. For example, the GDPR provides a clear timeline to provide information on action taken on a request within a period of 1 month of receipt of the request, which can be extended further by two months in circumstances where required, taking into consideration the complexity and number of the requests made.[108] Further, the extension along with the reason for the delay must be informed to the subject (the Data Principal).[109]

[104] DPDP Act, s.11(1).
[105] DPDP Rules, Rule 14(2).
[106] DPDP Rules, rule 14(5).
[107] DPDP Rules, rule 14(5).
[108] GDPR, Article 12(3).
[109] GDPR, Article 12(3).

1.1.2. Powers conferred on Investigating Agencies

Section 11(2) contains a significant carve out regarding accessing information about personal data which grants major powers to investigative agencies. Any requests made by the Data Principal pertaining to the identities of all other Data Fiduciaries/Data Processors and other information related to the personal data, shall not apply if such personal data was shared with a Data Fiduciary that is "authorised by law to obtain such personal data".[110] A data request is "authorized by law" when such sharing is pursuant to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.[111]This effectively invalidates the right to access information about personal data in Section 11(1) of the DPDP Act. with regards to sharing the data to any other Data Fiduciary that is authorised by law to obtain such personal data, where a written request is made for the objective of preventing, detecting, or investigating of offences or cyber incidents, or for prosecution or punishment of offences.

1.2. The Right to Correction and Erasure of Personal Data

The DPDP Act grants the Data Principal the following rights regarding the processing of personal data for which they had previously given consent, including consent voluntarily provided under Section 7(a) of the DPDP Act:[112]

a. the correction of their personal data;
b. the completion of their personal data;
c. the updating of their personal data; and
d. the erasure of their personal data.

If the Data Fiduciary receives a request for correction, completion or updating from a Data Principal, they shall:[113]

a. correct the inaccurate or misleading personal data;
b. complete the incomplete personal data; and
c. update the personal data.

A Data Principal shall make a request in the prescribed manner to the Data Fiduciary for their personal data's erasure.[114] It is important to note that requests for the erasure of a Data Principal's personal data are not automatically accepted and processed. The Data Fiduciary shall process and

[110] DPDP Act, s. 11(2).
[111] DPDP Act, s.11(2).
[112] DPDP Act, s.12(1).
[113] DPDP Act, s.12(2).
[114] DPDP Act, s.12(3).

complete requests, with two exceptions. These exceptions are when the retention of such personal data is necessary for a specified purpose *or* is necessary for compliance with any law.

1.3. The Right of Grievance Redressal

A Data Principal has the right to readily available means of grievance redressal provided by a Data Fiduciary or the Consent Manager.[115] Every Data Fiduciary and Consent Manager is expected to prominently publish its grievance redressal system on its website or app, or on both. Rule 14(3) provides for appropriate technical and organisational measures to be undertaken to ensure implementation.[116]

Scope of the grievance redressal mechanism: The grievance redressal mechanism is available in relation to *any act or omission* regarding the Data Fiduciary's/Consent Manager's performance of its obligations related to the Data Principal's personal data or their rights under the DPDP framework.[117]

Exhaustion of grievance redressal mechanism before approaching DPB: Section 13(3) provides that before the Data Principal approaches the DPB, they must exhaust the opportunity of redressing their grievance using the grievance redressal mechanisms of the Data Fiduciary or Consent Manager.[118]

Timeframe of response: Rule 14(3) sets a maximum 90 day timeframe for grievance redressal by any Data Fiduciary or Consent Manager from the date of its receipt for all/any class of Data Fiduciaries.

1.4. The Right to Nominate

A Data Principal under Section 14(1) of the DPDP Act has the right to nominate any other individual, who shall exercise the Data Principal's rights in the event of their death or incapacity. In this context, 'incapacity' has been defined to mean the inability to exercise Data Principal's rights on account of unsoundness of mind or infirmity of body. Further, this right is supported by Rule 14(4) of the DPDP Rules which provides that the Data Principal may nominate one or more individuals, in accordance with applicable law and the Data Fiduciary's terms of service, using the required means required and furnishing the necessary particulars.

While these rights are enshrined in the DPDP framework, there are several protections that exist in other data protection laws in the world which have not been included under the Indian

[115] DPDP Act, s. 13.
[116] DPDP Rules, rule 14(3).
[117] DPDP Act, s.13(1).
[118] DPDP Act, s.13(3).

framework. For instance, Article 82 of the GDPR provides for a right to compensation and liability.[119]

2. Duties of the Data Principal

The duties of a Data Principal under the DPDP Act, are as follows:[120]

1. to comply with the provisions of all applicable laws while exercising rights under the DPDP Act;
2. to not impersonate another person while providing their personal data for a specified purpose;
3. to not suppress any material information while providing their personal data for the following:
    a. any document issued by the State or any of its instrumentalities;
    b. unique identifier issued by the State or any of its instrumentalities;
    c. proof of identity issued by the State or any of its instrumentalities; or
    d. proof of address issued by the State or any of its instrumentalities.
4. to not register a false/frivolous grievance, complaint with a Data Fiduciary or the DPB; and
5. to furnish only verifiably authentic information while exercising the right to correction or erasure.

VII. EXEMPTIONS GRANTED TO DATA FIDUCIARIES

The DPDP Act has specified several exemptions to the obligations of Data Fiduciaries.[121] The exemptions create a gap of processing where the DPDP Act's core safeguards do not apply, leaving only two obligations: adherence to lawful processing under Section 8(1) and a general duty to implement *reasonable* security safeguards under Section 8(5). These are discussed briefly below.

1. Exemptions to Data Fiduciaries

Section 17 creates a broad exemption framework that carves out specific situations where key obligations under the DPDP Act, i.e. those in Chapter II (rights and duties), Chapter III (compliance requirements), and Section 16 (significant data fiduciaries), do not apply.[122]

[119] General Data Protection Regulation, Article 82.
[120] DPDP Act, s.15.
[121] DPDP Act, s. 17.
[122] DPDP Act, s.17.

These circumstances are as follows:

a. when the processing of personal data is necessary for enforcing any legal right or claim;
b. the processing of personal data by any court, tribunal or other body in India which performs any judicial, quasi-judicial, regulatory or supervisory function and where such processing is required for the functioning of such a body;
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 outside India is processed on account of a contract between any person outside India with any person based in India;
e. the processing is necessary for the restructuring of one or more companies by way of a a scheme of compromise, arrangement, merger, amalgamation of two or more companies, demerger, transfer of undertaking or involves the division of one or more companies as approved by a court or tribunal;
f. the processing of personal data is for determining the financial information, assets and liabilities of any person who has defaulted in a payment that was due owing to a loan/advance taken from a financial institution.

2. Analysis of the exemptions granted to Data Fiduciaries

2.1. Exemption for processing necessary to enforce legal rights or claims

Section 17(1)(a) creates a substantive exemption where the processing of personal data is necessary for enforcing any legal right or claim. This exemption applies across civil, criminal, and administrative proceedings, including litigation, arbitration, and any process before a court, tribunal, or statutory authority. Once the threshold of "*necessity*" is satisfied, the obligations of the DPDP Act do not apply to that specific processing operation.

The structure of the provision indicates that the exemption is purpose-bound rather than actor-bound: lawyers, litigants, arbitrators, and courts may all rely upon it, but only to the extent their processing is strictly required to enforce or defend a legal right. The phrase "*necessary for enforcing any legal right or claim*" is central, and in practice, courts may scrutinise this at the stage of discovery (facts[123] and documents[124]), inspection,[125] or when a party challenges the proportionality of a disclosure request. It is essential here that the Courts use their power on recognising necessity, proportionality, and minimal intrusion when privacy is implicated.

2.1.1. Use of Personal data in enforcing rights in civil and criminal proceedings

[123] Code of Civil Procedure 1908, Or 11 rr 1–11.
[124] Code of Civil Procedure 1908, Or 11 rr 12–14.
[125] Code of Civil Procedure 1908, Or 11 rr 15–19.

Personal data forms part of almost every legal dispute; financial records, communications, identification documents, employment data, IP logs, CCTV footage, and medical information often become material to establish facts. Section 17(1)(a) recognises this inevitability.

In criminal proceedings, courts and police officers may summon documents if they are necessary or desirable for investigation, inquiry, trial, or any proceeding.[126] The Supreme Court clarified in *CBI v. V. Vijay Sai Reddy, (2013),* observed that summons to produce documents must be used judiciously and in accordance with statutory safeguards.[127]

In civil cases, courts may require personal data to be disclosed when it is relevant to the dispute. Section 30 of the Code of Civil Procedure, 1908 empowers a court to order discovery, production, inspection, or return of documents.[128] These powers apply to any document that may assist the court in deciding the case, including documents that contain personal data.[129] The Supreme Court has held that the court must place strong emphasis on the truth of pleadings and documents, because truth is the foundation of justice.[130] In *Maria Margarida Sequeira Fernandes v. Erasmo Jack de Sequeira (2012)*, the Hon'ble Supreme Court observed that adherence to Section 30 of the Code of Civil Procedure, 1908 helps the court ascertain the truth and prevents dishonest litigation.[131]

In commercial suits, the obligation is even stricter. Order XI requires parties to file all documents in their possession, custody, or control that relate to the issues, even if the documents do not support their case.[132] Parties must also file a declaration on oath that no document has been withheld.[133] This is a continuing duty. Personal data often forms part of these documents, such as emails, financial details, or employment records. If a party refuses to disclose material documents, the court may draw an adverse inference or impose costs.[134]

2.2. Exemption for courts, tribunals, regulatory, supervisory bodies

Section 17(1)(b) creates an exemption for "the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, *where such processing is necessary for the performance of such function*" (emphasis supplied).

[126] Code of Criminal Procedure 1973, s. 91.
[127] *CBI v. V Vijay Sai Reddy*, (2013) 7 SCC 452.
[128] Code of Civil Procedure 1908, s. 30.
[129] Indian Evidence Act, 1872, s. 114(g); Sri Ram Industrial Enterprises Ltd v Mahak Singh AIR 2007 SC 1370.
[130] VR Krishna Iyer, 'Speech at the 18th Annual Conference of the American Judges Association, Seattle, Washington' (1979) 1 SCC (J) 7, 7.
[131] *Maria Margarida Sequeira Fernandes v Erasmo Jack de Sequeira,* (2012) 5 SCC 370.
[132] Commercial Courts Act 2015, s. 16.
[133] Code of Civil Procedure 1908, Order 11 r 3 (as amended by the Commercial Courts Act 2015).
[134] Code of Civil Procedure 1908, Order 11 r 6 (as amended by the Commercial Courts Act 2015).

The scope of this condition is central. Each authority derives its powers from a statute or from the Constitution. When the Act refers to necessity, the assessment must flow from (a) the statutory mandate of that body, (b) the purpose for which the law authorizes the function, and (c) whether the personal-data processing is required to achieve that purpose within the "four corners" of the law. For example, the Central Electricity Regulatory Commission (CERC)[135] may process personal data only to the extent permitted under the Electricity Act, 2003,[136] and applicable regulations. If the Commission processes personal data beyond statutory authority, or in a manner inconsistent with constitutional guarantees recognized in *K.S. Puttaswamy v. Union of India (2017)*,[137] such processing can be challenged for lack of legal basis or proportionality.

The phrase "*regulatory or supervisory function*" is broad and could include a wide range of statutory bodies across financial, economic, environmental, and administrative domains. Examples include:

a. Financial regulators such as Securities Exchange Board of India,[138] and Reserve Bank of India.[139]
b. Infrastructure and communications regulators such as Telecoms Regulatory Authority of India,[140] Central Electricity Regulatory Commission,[141] and the Airport Economic Regulatory Authority of India.[142]
c. Competition Commission of India.[143]
d. Environmental agencies such as State Pollution Control Boards, Central Pollution Control Board.
e. Adjudicatory tribunals such as National Company Law Tribunals, National Company Law Appellate Tribunal, Debt Recovery Tribunals, Debt Recovery Appellate Tribunal, and Telecoms Dispute Settlement Appellate Tribunal.

These bodies regularly process personal data while conducting investigations, adjudications, inspections, audits, show-cause proceedings, supervisory directions, and licensing actions. The DPDP Act now exempts all such processing if it is "*necessary*" for the statutory task. This means both adjudicatory functions (orders, hearings, penalties) and administrative or supervisory functions (market surveillance, inspections, prudential oversight) fall within the exemption.

[135] Electricity Act, 2003, s. 76.
[136] Electricity Act, 2003.
[137] *K.S. Puttaswamy I.*
[138] Securities and Exchange Board of India Act 1992, ch 2.
[139] Reserve Bank of India Act 1934, s. 3.
[140] Telecom Regulatory Authority of India Act 1997, s. 3.
[141] Electricity Act, 2003, s. 76.
[142] Airports Economic Regulatory Authority of India Act 2008; Government of India, 'Notification GSR 317(E)' (12 May 2009).
[143] Competition Act 2002, ch 3.

The justification for this type of exemption is the operational need for regulators and adjudicatory bodies to have unrestricted access to evidence, records, financial statements, metadata, call-detail records, and other types of personal data. Regulators frequently require this data to detect violations, enforce compliance, or conduct investigations. A regulator like SEBI may seek bank records, trading logs, KYC records, or phone records to trace insider trading.[144] RBI may examine borrower accounts or transaction histories for supervisory action.[145] Income-tax authorities may collect extensive financial and identity information during searches and assessments.[146] The intent of this exemption is that if such bodies were constrained by notice requirements, consent obligations, or deletion rights under the DPDP Act, their ability to enforce statutory mandates would be compromised.

Indian sectoral regulators already possess wide investigatory and data-collection powers under their governing statutes. The RBI's KYC and supervisory framework imposes comprehensive identity and transaction-recording obligations on regulated entities and permits sharing with credit information companies and supervisory agencies; these Directions do not impose strict, privacy-centric retention limits or a proportionality test equivalent to the *K.S. Puttaswamy - I* standard.[147] SEBI's powers to search, seize and access transactional records are similarly expansive and are used routinely in market-surveillance and fraud probes; the statute and practice focus on evidence-gathering rather than statutory privacy constraints.[148] Search-and-seizure provisions under the Income Tax Act, 1961, likewise allow extensive copying and retention of electronic and physical records.[149] While judicial review is available against arbitrary searches and seizures, the statutory scheme lacks explicit data-minimisation, deletion timelines, or privacy-specific retention obligations.

By exempting regulator-held processing from the DPDP Act where it is "*necessary for the performance of such function,*" Section 17(1)(b) effectively leaves the privacy consequences of statutory investigations to the governing sectoral laws. In practice this means that the privacy system of notice, purpose limitation, minimisation, storage limitation, and correction depends on whether the sectoral statute or regulator policy contains express safeguards. The DPDP Act and DPDP Rules do not impose uniform, cross-sectoral safeguards; the protection gap and the risk

[144] Securities and Exchange Board of India Act 1992, s. 11; *Sahara India Real Estate Corporation Ltd v. Securities and Exchange Board of India,* (2013) 1 SCC 1.
[145] Banking Regulation Act 1949, ss 21, 27, 30(1B), 35 and 35A; Reserve Bank of India Act 1934, ss 45B, 45C, 45JA, 45K and 45L.
[146] Income-tax Act 1961, ss 131, 132, 133 and 142.
[147] Reserve Bank of India, Know Your Customer (KYC) Directions 2016 (RBI Master Direction DBR.AML.BC.No.81/14.01.001/2015-16, 25 February 2016).
[148] Securities and Exchange Board of India Act 1992, s. 11C (inserted by Act 59 of 2002, s. 6, w.e.f. 29 October 2002).
[149] Income-tax Act, 1961, ss 131, 132, 133 and 142; Apar Gupta, Indumugi C., & Naman Kumar, India's new tax law raids your cloud, (Frontline, 30 August 2025), https://frontline.thehindu.com/news/income-tax-act-2025-digital-power-data-privacy-risks/article69992742.ece accessed 17 December 2025.

that sectoral priorities (market integrity, revenue collection, public safety) will trump privacy unless the sectoral law itself provides constraints.

2.3. Exemption for prevention, detection, investigation, or prosecution of offences

Section 17(1)(c) creates a broad exemption for any processing of personal data carried out for the prevention, detection, investigation, or prosecution of offences or legal contraventions. The wording is wide enough to include not only serious crimes but also minor statutory breaches, regulatory non-compliance, and administrative infractions. Once an authority invokes this exemption, the safeguards in Chapters II and III such as notice, consent, purpose limitation, accuracy, deletion, and the right to access do not apply. The exemption also does not require judicial approval, prior authorization, or a written assessment of necessity or proportionality. This contravenes the constitutional standards laid down in *K.S. Puttaswamy v. Union of India* (2017),[150] where the Supreme Court held that any restriction on privacy must satisfy the tests of legality, legitimate aim, proportionality, and procedural safeguards. In *Puttaswamy*,[151] The Supreme Court relied on *S. and Marper v. United Kingdom* (2008),[152] which held that indefinite retention of biometric and DNA data for investigative convenience violated privacy.

Indian courts have consistently tried to reinforce safeguards around State surveillance and investigative powers. In *Gobind v. State of M.P.* (1975),[153] the Supreme Court recognised that surveillance is a serious intrusion and upheld the law only by reading it narrowly. It stressed that privacy may be restricted only to meet a "compelling State interest" and that routine or unfounded surveillance is unconstitutional.[154] In *PUCL v. Union of India* (1997),[155] dealing with telephone tapping, the Supreme Court held that even when a statute authorises interception, additional procedural safeguards are necessary to make the intrusion fair, just, and reasonable. In *State of Maharashtra v. Bharat Shanti Lal Shah* (2008),[156] the Supreme Court upheld the MCOCA interception provisions only because they were narrowly tailored and contained strict safeguards.[157] In *Selvi v. State of Karnataka* (2010),[158] the Supreme Court held that involuntary narcoanalysis, polygraph tests, and BEAP tests violated privacy and the right against self-incrimination.[159] Similarly, in *Bhabani Prasad Jena v. Orissa State Commission for Women* (2010),[160] the Supreme Court observed that DNA testing ordered by a court must be allowed only after balancing privacy with the need for truth.[161] These judgments show that investigative

[150] *K.S. Puttaswamy I.*
[151] *K.S. Puttaswamy I, [*132].
[152] *S and Marper v. United Kingdom*, 2008 ECHR 151.
[153] *Govind v. State of Madhya Pradesh,* (1975) AIR 1378.
[154] *K.S. Puttaswamy I,* [380].
[155] *People's Union of Civil Liberties v. Union of India*, (1997) AIR SC 568.
[156] *State of Maharashtra v. Bharat Shanti Lal Shah*, (2008) 13 SCC 5
[157] *State of Maharashtra v. Bharat Shanti Lal Shah*, [60].
[158] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[159] *Selvi v. State of Karnataka*, [111].
[160] *Bhabani Prasad Jena v. Orissa State Commission for Women*, (2010) 8 SCC 633
[161] *Bhabani Prasad Jena v. Orissa State Commission for Women*, [86].

powers must be supervised, necessary, and proportionate. Section 17(1)(c) of the DPDP Act does not contain any of these constitutional safeguards.

The exemption under Section 17(1)(c) of the DPDP Act also creates risks of uncontrolled access and "function creep".[162] Without DPDP safeguards, authorities can demand personal data from telecom companies, social-media intermediaries, fintech entities, and banks without notice to the individual and without any restrictions on how the data may be reused. This creates parallel channels of access outside the CrPC,[163] the IT Act,[164] and the Telegraph Act[165] each of which contains at least *some* checks and oversight.

The danger of misuse is not theoretical.[166] In *Marcel v. Commissioner of Police* (UK, 1992),[167] the UK's Court of Appeal held that information obtained for one lawful purpose cannot be reused for a different, unrelated purpose. The German Federal Constitutional Court's *Census Case* (1983)[168] also recognised the threat posed by large State-controlled databases and developed the principle of informational self-determination.[169] Indian courts have recognised similar concerns. In *Girish Ramchandra Deshpande v. CIC* (2013), the Supreme Court held that personal information cannot be disclosed without necessity and proportionality.[170] Even the Supreme Court's judgment in *M.P. Sharma v. Satish Chandra* (1954), which is sometimes misunderstood as rejecting privacy, only held that a search is not the same as compelled testimony; it did not place searches beyond constitutional scrutiny.[171] Later surveillance cases, such as *PUCL,*[172] *Canara Bank*,[173] and finally *K.S. Puttaswamy I*,[174] have firmly located State searches and data collection within Article 21 and its fairness requirements. Unlike the GDPR, where law-enforcement data processing is governed by a separate and detailed Law Enforcement Directive (EU 2016/680),[175] the DPDP Act provides no equivalent framework. The result will be

[162] B-J Koops, 'The Concept of Function Creep' (2021) 13 *Law, Innovation and Technology* 29.
[163] Code of Criminal Procedure 1973, s. 91.
[164] *ITO v. Lakhmani Mewal Das,* (1976) 103 ITR 437.
[165] *P. Kishore v Secretary to Government*, 2025 SCC OnLine Mad 3053.
[166] NA Moreham, 'Police Investigations, Privacy and the *Marcel* Principle in Breach of Confidence' (2020) 12 *Journal of Media Law* 1.
[167] *Marcel v. Commissioner of Police*, [1992] Ch 225.
[168] BVerfGE 65, 1 (15 December 1983) § 145 (authors' translation).
[169] Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 *Computer Law & Security Review* 84.
[170] *Girish Ramchandra Deshpande v. Central Information Commr.,* (2013) 1 SCC 212 , [12].
[171] *M.P. Sharma v. Satish Chandra*, (1954) 1 SCC 385; See Gautam Bhatia, 'The Right to Privacy Hearing: Problems and Prospects' (*Constitutional Law and Philosophy*, 3 August 2017) https://indconlawphil.wordpress.com/2017/08/03/the-right-to-privacy-hearing-problems-and-prospects/ accessed 7 December 2025
[172] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301
[173] *District Registrar and Collector v. Canara Bank*, (2005) 1 SCC 496
[174] *K.S. Puttaswamy I.*
[175] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for criminal law purposes [2016] OJ L119/89.

a system where the most intrusive forms of State data processing receive the least statutory oversight.

This is also legitimizing intrusive access to personal devices of journalists in the garb of a criminal investigation. In 2022, a case titled *Foundation for Media Professionals v. Union of India* was filed before the Supreme Court of India, challenging the absence of any legal framework governing the search and seizure of electronic devices.[176] The petition showed that law-enforcement often compels individuals to unlock their phones without warrants or reasonable suspicion.[177] Foundation for Media Professionals argued that existing law under the CrPC only authorises search of "places" or seizure of "documents" or "things," none of which include digital records. On 18 October 2022, a Supreme Court Bench led by Justice K.M. Joseph issued notice in the matter and tagged it with an ongoing case titled, *Ram Ramaswamy & Ors. v. Union of India & Ors*.[178] In the said case, the Union Government had already filed a counter affidavit. Furthermore, the Supreme Court, on 7 November 2023,[179] acknowledged the seriousness of the issue and directed the Union Government to consider appropriate guidelines. The Central Government has not, to date, filed any appropriate guidelines before the Supreme Court of India.

Digital devices contain vast and intimate data that cannot be compared to physical "documents" or "things." Yet, police officers across India have stopped individuals on the street, demanded access to their phones, and extracted WhatsApp chats unrelated to the alleged offence.[180] These chats sometimes enter the public domain and are used for media trials.[181]

The absence of specific regulation has allowed law enforcement to treat personal devices as ordinary objects and to bypass warrant requirements. Foundation for Media Professionals

---

[176] *Foundation for Media Professionals v Union of India*, W.P. (Crl.) No 395/2022 (Supreme Court of India, pending).

[177] Umang Poddar, 'Can the police in India force someone to hand over their phone and check their messages?' (Scroll.in, 4 November 2021) https://scroll.in/article/1009529/can-the-police-in-india-force-someone-to-hand-over-their-phone-and-check-their-messages#:~:text=There%20is%20a%20constitutional%20protection,ones'%20right%20to%20remain%20silent. accessed 7 December 2025.

[178] *Ram Ramaswamy v Union of India*, W.P. (Crl.) No 138/2021 (Supreme Court of India, pending).

[179] *Foundation for Media Professionals v Union of India*, W.P. (Crl.) No 395/2022 (Supreme Court of India, order, 7 November 2023).

[180] Paul Oommen, 'Hyderabad cops are stopping people on the road, checking WhatsApp chats for 'drugs'' (The News Minute, 28 October 2021), Available at: https://www.thenewsminute.com/telangana/hyderabad-cops-are-illegally-checking-phones-whatsapp-citizens-part-drug-crackdown-156997 accessed 7 December 2025; Anirban Mitra, 'Kerala man alleges Bengaluru cop checked his WhatsApp, hidden photos in phone gallery' (The Indian Express, 27 November 2023) available at: https://indianexpress.com/article/trending/trending-in-india/kerala-man-alleges-bengaluru-cop-checked-his-whatsapp-hidden-photos-in-phone-gallery-9992443/ accessed 7 December 2025.

[181] Anirban Mitra, 'Bollywood drugs probe raises questions of digital privacy — here are the answers' (Indiatoday.in, 24 September 2020), available at: https://www.indiatoday.in/india/story/bollywood-drugs-probe-raises-questions-of-digital-privacy-here-are-the-answers-1725144-2020-09-24 accessed 7 December 2025.

therefore asked the Court to recognise that individuals cannot be compelled to reveal passwords, and that digital searches must meet the constitutional standard of proportionality.[182] Section 17(1)(c) of the DPDP Act moves in the opposite direction. It widens State power without placing any safeguards. By exempting the government from notice, consent, purpose limitation, and deletion obligations, it creates a real risk of normalising indiscriminate digital searches. The exemption therefore, threatens not only the privacy of ordinary citizens but also the safety of journalists, whistleblowers, and sources who rely on the confidentiality of digital communication.

2.4. Exemption for mergers, amalgamations, and corporate restructuring

Section 17(1)(e) of the DPDP Act creates an exemption for certain merger and acquisition transactions. The exemption applies only when the transaction is approved by a court, tribunal, or other competent authority. It covers schemes of compromise or arrangement, mergers and amalgamations,[183] corporate reconstruction including demergers,[184] and the transfer or division of undertakings. If a transaction falls within these categories and carries the required approval,[185] then this exemption will apply. However, all other M&A activity remains fully subject to the DPDP Act. For example, share-purchase transactions or private acquisitions that do not require court or regulatory approval cannot rely on this exemption. In those situations, the processing of personal data by any party, including a data processor, must comply with the full requirements of the DPDP Act.

This is different from the proposed framework under the DPDPB, 2022. Under the DPDPB, 2022, "deemed consent"[186] was recognised for all mergers, acquisitions, corporate restructurings, and similar transactions, as long as they complied with applicable law. That formulation was broader and automatically covered a wide range of M&A activity, regardless of whether the transaction required approval from any authority. In contrast, the DPDP Act adopts a narrower and more formal threshold, tying the exemption strictly to transactions that undergo judicial[187] or statutory scrutiny.[188] As a result, entities involved in private or informal restructuring must undertake compliance measures for any personal data processed during due diligence, valuation, or integration.

---

[182] *Supreme Court directs Union Govt. to contemplate laying down guidelines on Search and Seizure of Digital Devices*, Internet Freedom Foundation (7 November 2023) https://internetfreedom.in/supreme-court-requests-union-govt-to-contemplate-formulating-necessary-guidelines-on-search-and-seizure-of-digital-devices/ accessed [08.12.2025].
[183] Income Tax Act, 1961, s. 2(1B), .
[184] Income-tax Act 1961, s 2(19AA).
[185] Companies Act 2013, ss 230–232.
[186] Digital Personal Data Protection Bill, 2022, cl 8.
[187] Hologram Holdings Pvt Ltd and Swen Holdings Pvt Ltd with Sulphur Securities Pvt Ltd, CP (CAA) No 20/Chd/Hry/2022 (NCLT Chandigarh Bench, Second Motion, 23 July 2024).
[188] Companies (Compromises, Arrangements and Amalgamations) Rules 2016, r 25.

Even when the exemption applies, some duties continue. A data fiduciary cannot avoid its statutory obligations under Section 8(1).[189] It must also maintain reasonable security safeguards under Section 8(5).[190] These duties remain important because restructuring transactions involves large sets of personal data, including information about employees, customers, vendors, and contractors. The exemption does not remove the need for technical and organisational measures that protect personal data during negotiations, due diligence, and post-closing integration.

Some M&A transactions fall outside this exemption. Share purchases, asset sales, slump sales, business transfers, group reorganisations, and private acquisitions remain fully subject to the DPDP Act since you do not need the court's approval. In such cases, the buyer must map the personal data held by the target. It must examine the purpose of each processing activity. It must also review the target's compliance with sectoral regulations. Sector-specific rules in RBI,[191] SEBI,[192] IRDAI,[193] and others may impose additional duties. When the target operates in data-intensive sectors such as fintech, telecom, e-commerce, advertising, analytics, or AI, the privacy risks are higher. The DPDP Act and DPDP Rules influence how the buyer conducts due diligence and assesses the transaction.

Share sales and asset sales require different approaches.[194] In a share sale, the identity of the data fiduciary does not change. The company continues to control the data. The DPDP Act does not require fresh notice or consent unless the purpose or method of processing changes. In an asset sale, personal data moves from the seller to the buyer. This transfer changes the identity of the

[189] DPDP Act, s 8(1).
[190] DPDP Act, s 8(5).
[191] Reserve Bank of India Act 1934 and the rules and regulations framed thereunder, including: Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions 2023; Master Direction – Non-Banking Financial Company – Housing Finance Company (Reserve Bank) Directions 2021; Master Direction – Reserve Bank of India (Regulatory Framework for Microfinance Loans) Directions 2022; Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (7 November 2023); Master Direction – Core Investment Companies (Reserve Bank) Directions 2016 (applicable only to core investment companies); Asset Reconstruction Companies (Reserve Bank) Guidelines and Directions 2003 read with Master Circular – Asset Reconstruction Companies (applicable only to asset reconstruction companies); Master Circular – Prudential Norms on Income Recognition, Asset Classification and Provisioning pertaining to Advances; and Guidelines on Default Loss Guarantee (DLG) in Digital Lending.
[192] Securities and Exchange Board of India Act 1992, and the rules and regulations framed thereunder, including: Securities and Exchange Board of India (Substantial Acquisition of Shares and Takeovers) Regulations 2011; Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015; Securities and Exchange Board of India (Issue of Capital and Disclosure Requirements) Regulations 2018; and other sector-specific regulations such as the Securities and Exchange Board of India (Mutual Funds) Regulations 1996.
[193] Insurance Act 1938, and the rules and regulations framed thereunder, including: Indian Insurance Companies (Foreign Investment) Rules 2015; Insurance Regulatory and Development Authority of India (Registration of Indian Insurance Companies) Regulations 2022; IRDAI, Master Circular on Registration of Indian Insurance Company 2023; and Insurance Regulatory and Development Authority of India (Other Forms of Capital) Regulations 2022.
[194] Laura Myles and Nolene Treacy, Data Protection considerations when managing Mergers and Acquisitions ("M&A"), (Flynn O'Driscoll, 27 May 2021), https://www.fod.ie/news/data-protection-considerations-m-a accessed 16 December 2025.

data fiduciary. The parties must inform data principals, and in some cases, obtain fresh consent. Transaction documents must include representations, warranties, indemnities, and conditions precedent related to data-protection compliance.

Disclosure of personal data during due diligence is also serious. When a seller shares employee, vendor, customer, or contractor data with a potential buyer, the seller must comply with Section 6 of the DPDP Act on consent unless the activity fits within "legitimate use." Sharing limited employee information to assess continuity of employment may fall within legitimate use. However, the seller must still follow the principles of necessity and data minimisation and must restrict the handling of employee data to what is essential for the transaction's objectives.[195] The buyer must review the accuracy of the data, the involvement of third-party processors, the extent of international data transfers, and the company's arrangements with cloud providers and other vendors.

After closing the deal, cross-border data-transfer restrictions under other laws continue because Section 16(2)[196] does not override them. Transfers to third-party vendors or group entities may trigger fresh notice obligations. The buyer must update privacy policies, internal governance documents, and notices to data principals. Sellers and buyers often sign data-sharing or data-protection agreements to allocate responsibility for legacy data, retention periods, deletion duties, and contractual restrictions.

In practice, Section 17(1)(e) offers limited relief. As stated earlier, it helps only those transactions that require a statutory approval. It leaves many commercial M&A deals within the full scope of the DPDP Act. As a result, two similar transactions may receive different treatment based solely on whether they require court approval. The DPDP Act also provides no guidance on the handling of personal data during due diligence or integration. This creates uncertainty and fragments accountability. The exemption therefore illustrates a broader problem in Section 17. The DPDP Act relies on formalistic carve-outs instead of creating proportionate safeguards. This is producing gaps and inconsistencies that weaken the overall data-protection framework.

2.5. Exemption for ascertaining financial information of loan defaulters

Section 17 also creates a broad exemption for processing personal data to assess the financial position of a loan defaulter. The clause allows a financial institution to process a person's assets, liabilities, and related financial information once a default occurs, subject only to the disclosure norms contained in sectoral laws. The DPDP Act adopts the Insolvency and Bankruptcy Code

[195] Devina Somani, India's New Digital Personal Data Protection Laws & Its Implications For M&A Compliance, (The Corporate & Commercial Law Society Blog, HNLU), https://hnluccls.in/2024/02/23/indias-new-digital-personal-data-protection-laws-its-implications-for-ma-compliance/, accessed 16 December 2025.

[196] DPDP Act, s 16(2).

definitions of "default"[197] and "financial institution".[198] This clause treats credit recovery as a value that automatically prevails over the individual's right to privacy. It assumes that efficiency in recovering loans is more important than notice, consent, or proportional safeguards. This assumption is incorrect and poses legal risks because the Constitution does not recognise credit recovery as a value that overrides privacy by default.

The exemption is overbroad in scope and under-specified in safeguards. As worded it permits financial institutions to process "*personal data*" of defaulters without tying that processing to necessity, proportionality, or time-limits. Data processed for credit assessment often includes highly sensitive behavioural, transactional and derived profiling data; absent strict constraints, such processing can create persistent surveillance of economically vulnerable people and enable invasive downstream uses (credit scoring, targeted collections, merchant blacklists) that the DPDP Act otherwise should have prevented.

Section 17(1)(f) of the DPDP Act creates a structural conflict between the IBC's object of asset-maximisation and the DPDP Act's privacy framework. IP professionals and other IBC actors need clarity on how to handle personal data during insolvency. Without clear statutory rules, they face legal uncertainty, and data subjects face significant privacy harms. A balanced regime must recognise that insolvency does not extinguish privacy rights and that personal data cannot be auctioned like any other asset.

The Insolvency and Bankruptcy Code itself shows that insolvency does not remove the need for privacy safeguards.[199] Section 29(2)[200] requires resolution professionals to share information only after they receive confidentiality undertakings that protect business information and intellectual property. This requirement does not protect individual data subjects. It binds bidders not to leak data, but it does not impose any duty to delete, minimise, or limit the personal data that appears in the information memorandum.[201] This gap creates compliance risks for resolution professionals. If they remove personal data from an asset sale, they risk that they are reducing asset value. If they include personal data without DPDP safeguards, they risk violating privacy law and exposing themselves to liability under the DPDP Act.

In the Jet Airways insolvency in 2019,[202] the airline's loyalty-programme database became a contested asset.[203] Stakeholders treated passengers' identities, travel histories, and contact

[197] Insolvency and Bankruptcy Code 2016, s 3(12).
[198] Insolvency and Bankruptcy Code 2016, s 3(14).
[199] Insolvency and Bankruptcy Code, 2016.
[200] Insolvency and Bankruptcy Code 2016, s 29(2)
[201] Insolvency and Bankruptcy Code 2016, ss 25(2)(g) and 29.
[202] *Ashish Chhawchharia, Resolution Professional for Jet Airways (India) Ltd*, IA No 2081 of 2020 in CP (IB) No 2205/MB/2019 (NCLT Mumbai Bench, 22 June 2021).
[203] Jet Airways' stake in frequent-flyer scheme key for potential bidders, LiveMint (21 July 2019) https://www.livemint.com/companies/news/jet-airways-stake-in-frequent-flyer-scheme-key-for-potential-bidders-1563730990896.html accessed [08.12.2025].

information as a valuable property interest for potential acquirers. Under the DPDP Act, such a transfer would require a clear legal basis or consent. Insolvency cannot create consent. Absent express statutory limits, bidders could gain access to sensitive passenger data without the passengers' knowledge. This conflict demonstrates that insolvency value-maximisation cannot justify unrestricted access to personal data.

In *Southern Pacific Personal Loans Ltd* (2013),[204] the UK High Court held that liquidators hold personal data only as agents and must destroy it once it is no longer necessary for statutory duties. The UK High Court required them to honour data subject access rights and to retain only minimal information needed for creditor claims. The judgment establishes an important principle: insolvency does not erase data rights, and liquidators cannot treat personal data like a bankable asset. The European Union follows the same approach. Article 5 of the GDPR requires fairness, purpose limitation, and legal basis for any transfer.[205] EU regulators blocked transfers of customer data in the Thomas Cook insolvency because insolvency did not override the need for user consent.[206]

In Europe personal data attaches to the person, not the company, and therefore cannot be freely sold.[207] The same principle applies in India as well. Insolvency law aims to maximise value for creditors, but the DPDP Act and the Constitution treat personal data as an extension of individual autonomy. The right to informational privacy recognised in *K.S. Puttaswamy* I[208] requires strong justification before the State or private actors interfere with data rights. Section 17(1)(f) of the DPDP Act ignores this constitutional framework. It creates a risk that insolvency professionals may treat personal data as an asset to monetise, even though the DPDP Act and the Constitution require strict necessity, proportionality, and purpose limitation. Insolvency law cannot override these safeguards unless Parliament states clear limits and ensures protection of rights.

3. Exemptions to the State and its Instrumentalities

Section 17(2)(a) of the DPDP Act grants exemption from the application of its provisions entirely to the processing of personal data to State instrumentalities as notified by the Central Government in the following situations:[209]

a. in the interests of sovereignty and integrity of India;
b. security of the State;
c. friendly relations with foreign States;

[204] Re Southern Pacific Personal Loans Ltd. 2013 EWHC 2485 (Ch).
[205] Regulation (EU) 2016/679 (General Data Protection Regulation) art 5.
[206] Re Thomas Cook Group plc and others [2019] EWHC 2626 (Ch).
[207] Ronny Hauck, 'Personal Data in Insolvency Proceedings: The Interface between the New General Data Protection Regulation and (German) Insolvency Law' (2019) 16 European Company and Financial Law Review 724, doi:10.1515/ecfr-2019-0024.
[208] *K.S. Puttaswamy I.*
[209] DPDP Act, s.17(2)(a).

d. maintenance of public order;
e. preventing incitement to any cognizable offence regarding the above offences; and
f. the processing of any personal data by the Central Government that such a State instrumentality furnishes to it.

With regards to the processing of personal data by the State or any State instrumentality, the provisions of pertaining to correction or erasure of personal data on the request of the Data Principal shall not apply,[210] where such processing is for a purpose that excludes decision-making that affects the Data Principal.[211]

4. Analysis of the exemptions to the State and its Instrumentalities for State schemes and frontline workers

Section 17(2)(a)[212] states:

> *"The Central Government may, by notification… exempt any instrumentality of the State from the application of the provisions of this Act* ***in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order*** *or preventing incitement to the commission of any cognisable offence."*

This text gives the Central Government the power to exclude an entire instrumentality of the State from all obligations under the DPDP Act, not merely from specific provisions. The DPDP Act does not define "*instrumentality of the State,*" and therefore the term follows the broad meaning developed under Article 12, which includes ministries, departments, statutory bodies, public sector undertakings, autonomous agencies, and other bodies delivering welfare schemes and public functions of the State.[213]

The provision does not require the Government to publish reasons, demonstrate necessity, or establish proportionality. It only requires the Government to issue a notification. Because the DPDP Act uses the phrase "may, by notification… exempt any instrumentality of the State", the power is discretionary and unbounded by procedural safeguards. The DPDP Act also does not require the Government to review such notifications periodically. The DPDP Rules do not impose any procedural checks on exemptions issued under Section 17(2). No Rule addresses publication of reasons, time limits on exemptions, or oversight mechanisms. A single executive notification can therefore remove entire public institutions and databases from the scope of the DPDP Act.

[210] DPDP Act, s.8(7), 12(2), 12(3).
[211] DPDP Act, s. 17(4).
[212] DPDP Act, s 17(2)(a).
[213] Constitution of India, art 12.

This exemption has significant consequences for welfare schemes because these systems depend on the ongoing collection of large volumes of personal data. Schemes such as ICDS[214] and POSHAN[215] gather child health records, pregnancy data, immunisation details, and family information. Programs such as PM-JAY[216] and DBT[217] collect identity documents, bank account details, caste certificates, and household profiles. If the Ministry of Women and Child Development, the National Health Authority, State Social Welfare Departments, or their implementing agencies are exempted under Section 17(2)(a), these large databases will no longer be bound by the core protections afforded to Data Principals in the DPDP Act. In such a situation, the State would not need to issue notices, obtain consent, ensure purpose limitation, delete unnecessary data, correct inaccurate records, or provide access rights to beneficiaries.[218] Millions of individuals would be placed in a system where they must hand over personal data to receive essential public benefits but do not receive any privacy protection in return. Because welfare schemes are not voluntary, this creates a major imbalance of power between the individual and the State.

The exemption also directly affects Anganwadi workers.[219] They gather sensitive information on children, pregnant women, and families and upload it into centralized databases such as the Poshan Tracker.[220] If Section 17(2)(a) of the DPDP Act exempts the supervising ministry or department, then Anganwadi workers will continue collecting this data without any statutory duty on the State to minimise the data collected, ensure accuracy, restrict retention, or put in place strong security safeguards. Beneficiaries will not receive notices or know how their information is stored, used, or shared. The absence of DPDP Act obligations leaves Anganwadi workers operating inside an unregulated data ecosystem, often with limited training and inadequate infrastructure. This raises systemic risks for women and children whose sensitive information can be stored indefinitely and shared across departments without their knowledge.

---

[214] Integrated Child Development Scheme (ICDS), Child Development Manual for District-Level Functionaries (Ministry of Women and Child Development 2017).

[215] Press Information Bureau, '[Nourishing the Nation Poshan Abhiyan's Holistic Approach to Nutrition and Wellness]' (PIB, <d07 MAR 2025>)https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2109222 accessed 8 December 2025.

[216] Ministry of Health and Family Welfare, '4.5 crore families to be benefitted' (Press Release, MoHFW, 25 July 2024) https://www.mohfw.gov.in/?q=/press-info/7742 accessed 8 December 2025.

[217] Press Information Bureau, 'India's DBT: Boosting Welfare Efficiency' (21 April 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2123192 accessed 8 December 2025.

[218] DPDP Act, s. 5, 6, 8, 11-13, 15.

[219] Misbah Rashid, 'ASHA, Anganwadi workers to collect data on people above 70 yrs of age to bring them under government health scheme' (LiveMint, 30 March 2021) https://www.livemint.com/politics/policy/asha-anganwadi-workers-to-collect-data-on-people-above-70-yrs-of-age-to-bring-them-under-government-health-scheme-11718100020760.html accessed 8 December 2025.

[220] Press Information Bureau, 'Under Saksham Anganwadi and Mission Poshan 2.0, IT systems leveraged to strengthen and bring transparency in nutrition delivery support systems: Poshan Tracker facilitates monitoring and tracking of AWCs, Anganwadi Workers and beneficiaries on defined indicators' (PIB Delhi, 5 December 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2199403 accessed 8 December 2025.

The exemption also removes transparency and accountability. Section 17(2)(a) does not require the Government to publish a list of exempted bodies, describe the types of data processed, specify the duration of the exemption, or notify data principals whose information falls outside the DPDP Act. The DPDP Rules do not cure these gaps. The result is a broad zone of administrative opacity that contrasts sharply with global data-protection frameworks. In the EU, for example, exemptions under Article 23 of the GDPR[221] must satisfy strict necessity, proportionality, documentation, and oversight requirements. India's framework contains none of these safeguards. Exemptions can also be justified on vague grounds such as "public order", which the DPDP Act does not define and which has no operational tests under the DPDP Act or DPDP Rules. This makes it possible for the executive to exempt welfare databases without having to meet constitutional standards.

In *K.S. Puttaswamy I,*[222] the Supreme Court held that privacy is a fundamental right and that any restriction on it must satisfy the tests of legality, legitimate aim, necessity, and proportionality. Section 17(2)(a) of the DPDP Act fails to incorporate these requirements. It permits the executive to set aside the entire privacy framework through subordinate legislation without parliamentary oversight or judicial scrutiny. This is especially troubling in welfare schemes, where participation is essential for survival and individuals cannot meaningfully refuse data collection. When the State manages the data of women, children, low-income households, and other vulnerable groups, privacy protections should be stronger; Section 17(2)(a) reverses this completely. It creates a legal regime in which welfare data can be processed without consent, without rights, and without accountability. This shifts the balance of power dramatically in favour of the State and undermines the constitutional vision of privacy as a safeguard against unrestrained state surveillance.

5. Exemption for Research Purposes

Section 17(2)(b) of the DPDP Act grants exemption from the application of its provisions entirely to the processing of personal data necessary for research, archiving, or statistical purposes.[223] This provision states that an exemption for research is applicable so long as the personal data is not used to make any decision regarding a Data Principal and such processing is carried out as per the prescribed standards in Second Schedule to the DPDP Rules.

6. Analysis of exemptions granted for research purposes

Section 17(2)(b) of the Digital Personal Data Protection Act, 2023 creates a broad exemption and states that the Central Government may, "by notification and subject to such terms and conditions as may be specified, exempt any data fiduciary or class of data fiduciaries from the application of the Act for research, archiving or statistical purposes." Rule 16 of the DPDP Rules, 2025

[221] Regulation (EU) 2016/679 (General Data Protection Regulation), art 23.
[222] *K.S. Puttaswamy I.*
[223] DPDP Act, s.17(2)(b).

operationalises this power. It states that processing for "research, archiving or statistical purposes" may be carried out without complying with obligations relating to notice, consent, accuracy, retention, disclosure, or the rights of data principals, provided that (i) the processing is not used for decision-making affecting individuals, and (ii) the processing meets the government's prescribed standards of anonymisation or de-identification. In effect, Section 17(2)(b) read with Rule 16 permits large-scale use of personal data for research without consent and without the safeguards ordinarily applicable to personal data processing. This creates a zone where the State may entirely suspend the application of the DPDP Act for categories as broad and undefined as "research" or "archiving", leaving wide discretion to executive notification.

The Supreme Court in *K.S. Puttaswamy I*, recognised that research purposes may justify a limited restriction of privacy but only within a carefully balanced framework. The Court held that the "*right to be forgotten*" cannot be exercised where data is necessary "*for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.*"[224] At the same time, the Supreme Court emphasised that these exceptions justify restrictions in all cases of breach of privacy, including breaches of data privacy only because they rest on legitimate public purposes and are subject to proportionality. Thus, the Supreme Court viewed research-related exemptions as narrow, purpose-bound, and subject to constitutional scrutiny, not as a blanket permission to escape regulatory oversight.

The Supreme Court explicitly warned that data-protection frameworks must ensure that the State cannot use research as a pretext to avoid consent or expand access to personal information. The Supreme Court acknowledged the public benefit of scientific and historical research based on data collected and processed. The Supreme Court added that the State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed.[225] Thus, the Supreme Court made it clear that processing for research purposes must remain purpose-limited, consent-respecting, and subject to privacy safeguards. Section 17(2)(b) of the DPDP Act and Rule 16 of the DPDP Rules depart substantially from these constitutional principles by granting complete exemption rather than designing calibrated safeguards.[226] As a result, the exemption for research purposes risks enabling broad State access to personal data without consent, transparency, or accountability precisely the outcome the Supreme Court warned against.

7. Ancillary Powers of the Central Government regarding Exemptions

a. **Exemptions for notified entities such as start-ups:** Under Section 17(3) of the DPDP Act, the Central Government is empowered to notify certain Data Fiduciaries or class of Data Fiduciaries in respect of whom Section 5 (Notice), Sections 8(3) and 8(7) (certain General

[224] *K.S. Puttaswamy I.,* p. 631.
[225] *K.S. Puttaswamy I.,* p. 631
[226] DPDP Act, s.17(2)(b); DPDP Rules, rule 16.

Obligations of the Data Fiduciary), Section 10 (Additional obligations of Significant Data Fiduciary), and Section 11 (right of the Data Principal to access information about personal data) of the DPDP Act shall not be applicable.[227] Such Data Fiduciaries include, for instance, start ups.

b. **Exemption for State/instrumentalities where the decision will not affect Data Principal:** Section 17(4) provides a further relaxation for processing carried out by the State or its instrumentalities, exempting them from Section 8(7), Section 12(3), and Section 12(2), where no decision affecting the Data Principal is involved.[228]
c. **Declaring an exemption from the provisions of the DPDP Act any time before 13 November 2030:** As per Section 17(5), before the conclusion of five years from the date of commencement of the DPDP Act (i.e. any time before 13 November 2030), the Central Government has the authority to declare that a Data Fiduciary or a class of Data Fiduciaries shall be exempted from any provision under the DPDP Act.[229]

8. Potential for abuse under Section 17(4) of the DPDP Act

Section 17(4) of the DPDP Act exempts State or its instrumentalities from the obligations concerning erasure and/or correction of data.[230] In practice this means the State or its instrumentalities need not erase data when the specified purpose ends. It also means the State or its instrumentalities can refuse requests to erase or, in many cases, to correct inaccurate data.

This is enabling indefinite retention by the State and its instrumentalities. Old records include administrative allegations, health records, beneficiary lists and surveillance logs. Indefinite retention turns data into permanent dossiers. Permanent dossiers enable retrospective profiling, reputation harm, and mistaken decisions long after the original purpose has passed.

The inability to demand correction amplifies harm from errors. Government databases often contain mistakes, wrong dates, mis-tagged names, wrong identity numbers, or incorrect categorizations. Section 17(4) of the DPDP Act prevents a person from forcing correction in many routine state processes. A minor error can therefore block welfare benefits, deny clearances, skew criminal background checks, and ruin employment prospects. The law thus formalizes the "data double" that the person cannot repair.

This exemption also encourages function-creep. Data collected for a limited administrative function can be repurposed for other purposes.[231] A health survey can feed into welfare eligibility lists or law-enforcement intelligence. Because the State and its instrumentalities do not have to erase or delete data when decisions made pursuant to such data do not affect the Data Principal,

[227] DPDP Act, s. 17(4).
[228] DPDP Act, s. 17(4)
[229] DPDP Act, s.17(5).
[230] DPDP Act, s. 17(4).
[231] B J Koops, 'The Concept of Function Creep' (2021) 13 Law, Innovation and Technology 29.

the cost of repurposing is low. Agencies can test new uses without the friction that privacy safeguards normally create.

This provision invites aggregation and inter-agency sharing without constraints. When the State or its instrumentalities do not have to erase data, multiple agencies can pool legacy records to create richer profiles. Those profiles can drive automated risk scores, predictive policing, eligibility algorithms, and social-credit style monitoring. The law imposes no proportionality test, no independent review, and no mandatory retention limit to restrain such aggregation.

Section 17(4) of the DPDP Act conflicts with the proportionality principle established by *K.S. Puttaswamy I*.[232] The Supreme Court observed that State intrusions must be necessary, proportionate and subject to safeguards. A blanket statutory bar on erasure and correction for all State processing does not calibrate the interference to the nature of the interest involved. The exemption should be narrow, time-bound, and tied to demonstrable legal need. Presently, it reads as a broad delegation of power without the minimum safeguards.

The exemption also weakens accountability and remedies. If a public authority refuses to erase or correct any data, the affected person must turn to the Data Protection Board or the courts. However, the Data Protection Board may itself be structurally dependent on the State. Effective accountability requires immediate administrative remedies: a rapid internal review mechanism, transparent reasons for refusal, and interim corrective steps while disputes are pending.

In short, Section 17(4) of the DPDP Act hands the State a powerful exemption that removes deletion and correction rights. That exemption creates clear risks of indefinite retention, error-driven harm, mission-creep, aggregation, chilling effects on dissent, and weak accountability.

VIII. POWER TO CALL FOR INFORMATION

Section 36 of the DPDP Act states that the Central Government may require the DPB, any data fiduciary, or intermediary to provide information that it may call for.[233] Even though this provision does not state that rules may be prescribed under it, Rule 23 of the DPDP Rules requires furnishing information pertaining to the purposes listed in Seventh Schedule of the DPDP Rules, within the specified period as may be given in such.[234] Such information requests must be routed through the corresponding authorised person indicated in the Seventh Schedule of the DPDP Rules.[235]

[232] *K.S. Puttaswamy I.*
[233] DPDP Act, s. 36.
[234] DPDP Rules, rule 23.
[235] DPDP Rules, rule 23(1).

1. Purposes for which information may be called for

The purposes for which the Central Government may call for information from a Data Fiduciary or an intermediary and require them to furnish such information, are as follows:

a. in the interest of sovereignty and integrity of India or security of the State;
b. performance of any function under any law;
c. disclosure of any information for fulfilling any obligation under any law;
d. carrying out assessment for notifying any Data Fiduciary or class of Data Fiduciaries as SDF.

SEVENTH SCHEDULE

[*See* rule 23(1) and 8(3)]

S. no.	Purpose	Authorised person
(1)	(2)	(3)
1.	Use, by the State or any of its instrumentalities, of personal data of a Data Principal in the interest of sovereignty and integrity of India or security of the State.	Such officer of the State or of any of its instrumentalities notified under clause (a) of sub-section (2) of section 17 of the Act, as the Central Government or the head of such instrumentality, as the case may be, may designate in this behalf.
2.	Use, by the State or any of its instrumentalities, of personal data of a Data Principal for the following purposes, namely: — (i) performance of any function under any law for the time being in force in India; or (ii) disclosure of any information for fulfilling any obligation under any law for the time being in force in India.	Person authorised under applicable law.
3.	Carrying out assessment for notifying any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary.	Such officer of the Central Government, in the Ministry of Electronics and Information Technology, as the Secretary in charge of the said Ministry may designate in this behalf.

2. Bar on Disclosing Sharing of Information

Further, the Rule also stipulates that where the disclosure that such information (personal data) is itself likely to "prejudicially affect the sovereignty and integrity of India or security of the State", the Data Fiduciary or the intermediary will be barred from disclosing that they have shared such information to the Data Principal who is affected, or to any other person unless they are permitted do so by relevant authorised person in writing.[236]

3. Analysis

Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules effectively grants sweeping powers to the Central Government along with exempting them from complying with several important provisions regarding the processing of personal data under the DPDP Act.[237] The structural scaffolding of these provisions positions them as crucial requirements for law enforcement and governance. However, these provisions have grave potential for misuse given

[236] DPDP Rules, rule 23(2).
[237] DPDP Act, s. 36; DPDP Rules, rule 23.

that they are broad, vague, and are devoid of any procedural guardrails. This raises concerns of potential State overreach given that personal data can be called for by the State in an arbitrary manner without any explicit and enforceable limits.[238] Further, the provision does not include a mechanism for a formal, written request by the Central Government when calling for information from Data Fiduciaries or intermediaries, which once again highlights issues of arbitrariness and potential misuse of power.[239]

Thus, while the overarching objective of the legal framework for data protection under the DPDP Act and DPDP Rules is purportedly to protect the digital personal data of individuals along with placing limits on the processing of data for lawful purposes, wide ranging powers such as granted under Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules decidedly skews the balance in the favour of the State, without providing for any accountability.[240]

Further the bar on Data Fiduciaries and intermediaries on disclosing that they have furnished digital personal data to the Central Government when called upon to do so likely to "prejudicially affect the sovereignty and integrity of India or security of the State" is alarming as well, on similar grounds of it being broad and arbitrary.[241]

In *Maneka Gandhi v. Union of India* (1978), the Supreme Court held that procedures which are related to restricting a fundamental right must be designed in a careful manner and eliminate anything "arbitrary, freakish or bizarre".[242] Further, in *People's Union of Civil Liberties v. Union of India and Anr.* (1997), the Supreme Court held that it was necessary to lay down procedural safeguards to ensure that the right to privacy of a person is protected.[243] Rule 23 of the DPDP Rules accords unfettered power without any limitations or oversight circumventing the bulwark laid down by the Court in PUCL which had held that intercepting communications infringed the right to life and liberty guaranteed under Article 21 of the Constitution of India except when done through a procedure established by law.

One of the key principles highlighted in *K.S. Puttaswamy I* was 'purpose limitation', a critical principle of data protection which necessitates that data that is collected for a particular purpose cannot be used for any other objective. However, vaguely worded provisions in the law granting

[238] Rubayya Tasneem and Injila Muslim Zaidi, The Draft Digital Personal Data Protection Rules: Surveillance For Surveillance's Sake, The Wire, 16 January 2025, available at: https://thewire.in/rights/draft-dpdp-rules-surveillance-for-surveillances-sake/?ref=static.internetfreedom.in ["**Tasnmeen and Zaidi**"].
[239] Ibid.
[240] Krishna Preetham Kanthi, Privacy, Surveillance, and State Interest: Appraising the DPDP Act through a Constitutional Perspective, Indian Journal of Law and Technology (IJLT) Blog, 12 April 2025, available at: https://forum.nls.ac.in/ijlt-blog-post/privacy-surveillance-and-state-interest-appraising-the-dpdp-act-through-a-constitutional-perspective/.
[241] Tasneem and Zaidi.
[242] *Maneka Gandhi v. Union of India,* 1978 AIR 597.
[243] *People's Union of Civil Liberties v. Union of India and Anr.* (1997)

broad exemptions to the State and its instrumentalities undermine this principle, by permitting unlimited usage of data which goes beyond the principle's original intent.[244]

In addition to this, it is essential that the collection of personal data fulfils the principle of proportionality as highlighted in *K.S. Puttaswamy I* as well which effectively means that the State and its instrumentalities must justify the necessity and proportionality of their action of calling for such digital personal data from Data Fiduciaries and/or intermediaries.[245] Thus, unquestioned permission to gather data cannot be condoned and a legal framework for data protection must have specific and targeted laws which guarantee that data is collected and retained only for legitimate purposes.

These provisions allow the Central Government to demand access to personal data held by civil society organisations, NGOs, and service providers. The reasoning to request the data is national security, public order, and law enforcement, these powers create an environment of routine data extraction and surveillance. Organisations that work with vulnerable communities such as migrants, informal workers, tribal groups, or recipients of welfare schemes can be compelled to disclose sensitive information that beneficiaries shared only for service delivery, not for State monitoring.

Many welfare and community beneficiaries interact with NGOs precisely because they lack formal identification, stable housing, or digital access.[246] When organisations are legally required to collect identity details, maintain logs, and be prepared to turn over data upon request. This expands the State's visibility into their lives, often without their informed understanding or meaningful ability to refuse.

For government welfare beneficiaries, these provisions create a chilling effect. Beneficiaries of food security schemes, health programmes, pension systems, or social protection services may avoid seeking help from civil society organisations if they fear their data may reach government authorities. This is serious for communities that already face harassment such as street vendors, refugees, sex workers, undocumented migrants, or individuals in conflict with local authorities. When people know their interactions, grievances, or personal information can be accessed by the government, they may choose silence over support.

The requirement to provide clear, itemised notices and obtain informed consent also becomes a barrier in the context of welfare. Many beneficiaries are not literate, do not understand digital data practices, or fear engaging with formal processes. Asking them to sign or digitally accept

[244] Daniel J. Solove, A Taxonomy of Privacy, (2006) 154(3) University of Pennsylvania Law Review 477.

[245] The Internet Freedom Foundation, Detailed Submission on Behalf of the Internet Freedom Foundation to the Draft Digital Personal Data Protection Rules", 4 March 2025, available at: https://internetfreedom.in/iffs-response-to-meity-on-the-draft-data-protection-rules/.

[246] L Doshmangir, A Sanadghol, E Kakemam and R Majdzadeh, 'The involvement of non-governmental organisations in achieving health system goals based on the WHO six building blocks: A scoping review on global evidence' (2025) 20 PLoS One e0315592.

consent forms can be perceived as a risk, particularly when identity information is involved. This undermines trust, reduces access to welfare services, and weakens the ability of civil society to act as an intermediary in delivering rights.

IX. IMPLICATIONS OF INDIA'S DIGITAL PERSONAL DATA PROTECTION FRAMEWORK FOR CIVIL SOCIETY MEMBERS

1. Increase in surveillance, identification requirements, and implications for government beneficiaries

The DPDP Act and DPDP Rules introduce a compliance framework that significantly increases the State's visibility into individuals' personal data. The key mechanism is the expansive power granted to the Central Government under Section 36, which authorises it to demand access to any personal data held by organisations, including civil society organisations (CSOs) and nonprofits. The Draft Rules extend this power by allowing authorities to obtain data without any procedural safeguards, judicial review, or independent oversight. This marks a structural shift: organisations that were previously trusted intermediaries between vulnerable communities and the State are now placed in a position where they can be compelled to act as data suppliers to the government.

DPDP Act increases the surveillance environment around welfare delivery. People approach CSOs precisely because they seek confidentiality, discretion, and support. Once organisations are compelled to maintain data in a manner that ensures it can be inspected or demanded, the boundary diminishes between welfare support and state surveillance. If beneficiaries believe that approaching an NGO for help with pensions, scholarships, health benefits, or grievance redressal will result in their personal data being shared with authorities, the trust that enables welfare access breaks down. People who fear adverse consequences such as undocumented migrants, people with pending police matters, or those who face caste-based discrimination at local levels may choose to avoid interactions altogether.

The compliance burden also forces organisations to systematically collect more data than necessary, especially identity-related documents. Because they must now provide detailed notices, retain proof of consent, maintain logs, and be accountable for "verifiable requests," CSOs may default to collecting Aadhaar cards, ration cards, birth certificates, medical records, or parental verification documents even when these were previously unnecessary for delivering the service. This shift is not driven by service needs but by defensive compliance, stemming from the fear of penalties and unlimited government data procurement powers.

This directly increases the need for identification even when identification itself is a barrier. Many beneficiaries such as urban homeless persons, people living in informal settlements, migrant workers, refugees, sex workers, transgender persons, unaccompanied minors, or individuals fleeing violence do not possess uniform or updated formal identification. When CSOs

are compelled to gather identity information from such groups, beneficiaries may withdraw from support systems altogether. For vulnerable communities, identification is not merely an administrative hurdle; it is a source of risk. Being asked for ID can trigger fears of police reporting and profiling, immigration-related surveillance, or loss of anonymity for eg. HIV treatment, trafficking rescue operations, or gender-based violence counselling.

The requirement of formal, "itemised" notices and informed consent while essential in principle becomes counterproductive in the context of assisting in welfare where beneficiaries often lack literacy, digital familiarity, or the capacity to navigate formal data disclosures. The act of providing a legal notice to a daily-wage worker, a distressed woman, or a person in a humanitarian crisis transforms a service interaction into an administrative process. Many beneficiaries may perceive the consent form as something that ties them to government monitoring or exposes them to future scrutiny. This creates confusion, fear, and disengagement. Rather than empowering individuals, these requirements may unintentionally erect barriers to receiving help.

For organisations themselves, the compliance burden shifts their focus. Time and resources that previously went into service delivery, legal empowerment, food distribution, rescue operations, or community organising must now be diverted to drafting notices, obtaining signatures, maintaining audit logs, documenting consent flows, training volunteers, and preparing for potential government demands. Small or resource-constrained CSOs will find this transition unmanageable, especially those operating with volunteers or informal community networks. Some may choose to reduce data collection altogether, while others will retreat due to resource constraints.

The cumulative effect is a systemic redistribution of power: the State gains more controlling power, CSOs gain more obligations, and beneficiaries lose anonymity, safety, and trust. The DPDP framework therefore, not only regulates data but restructures welfare ecosystems. It heightens surveillance, forces identification where it was previously unnecessary or harmful, and risks pushing the most vulnerable communities into further invisibility by making them wary of seeking help. What begins as a data protection requirement ultimately becomes a mechanism that deepens existing inequalities and increases the State's control over people who already experience unnecessary scrutiny.

2. Compliance pressure for non-profits and CSOs

For non-profits and CSOs, the DPDP Act creates many structural challenges because these entities operate under constraints and the DPDP Act and DPDP Rules does not recognise them: limited staff capacity, donor-driven budget cycles, volunteer-based operations, and work with vulnerable populations who cannot meaningfully navigate formal notice-and-consent frameworks. The DPDP Act requires CSOs to issue detailed notices, obtain explicit and

demonstrable consent, maintain logs, document data flows, and respond to access/deletion requests even where their interactions with beneficiaries occur in crisis situations or humanitarian contexts where formal documentation is impractical or harmful.

Many non-profits do not maintain sophisticated IT systems (due to budget constraints). Their data is often stored across spreadsheets, shared drives, WhatsApp groups, or cloud platforms used by volunteers. Converting these decentralised systems into a structured, auditable, and policy-compliant data sheet demands resources far exceeding the average operational budgets of grassroots organisations. Even medium-sized NGOs with professional staff lack the financial or technical capacity to design deletion workflows, track data minimisation, or implement access-control mechanisms. The compliance standards in the Act can only be achieved by large, well-funded NGOs, further widening inequality within the sector.

Moreover, the DPDP Act does not recognise vulnerabilities of organisations working in different sectors. Organisations working in domestic violence, child protection, labour rights, gender justice, migrant worker support, HIV treatment, trafficking rescue, and humanitarian relief rely on discretion and minimal documentation as a protective measure for beneficiaries. The requirement of formal notices and consent protocols can undermine trust, introduce fear, and deter people from seeking help. This collision between legal compliance and caregiving places CSOs in an impossible position: comply with the DPDP Act and risk endangering beneficiaries, or prioritise beneficiary safety and risk statutory penalties.

The absence of exemptions for nonprofits is a significant failure on the part of the legislature. Unlike many other jurisdictions that classify humanitarian, welfare, or public-interest organisations under specific low-risk categories, the DPDP Act applies a single compliance template to all entities. One glove can fit all approaches against Article 21. This leads to several adverse outcomes. First, organisations may begin collecting more identity data than necessary merely to safeguard themselves from future compliance liabilities, ironically increasing risk rather than reducing it. Second, CSOs may reduce the scope of their fieldwork or cease certain sensitive programmes where data could expose beneficiaries to harm. Third, donor agencies, especially foreign funders, may require NGOs to demonstrate full DPDP compliance before releasing funds, adding new layers of bureaucratic burden.

Finally, the government's power under Section 36 to demand access to personal data without judicial oversight directly affects nonprofits working with communities facing state actions, such as human rights defenders, minority groups, migrant workers, or protest-affected populations. These organisations must now treat all collected data as potentially subject to state requisition, fundamentally altering the trust relationship with the communities they serve. When CSOs become compelled data intermediaries, the space for independent civil society shrinks, and beneficiaries lose safe space where they can seek support without fear of surveillance.

X. AMENDMENT TO THE RTI ACT AND LACK OF JOURNALISTIC EXEMPTION

This section considers the impact of the amendments made by the DPDP Act to the RTI Act, and the lack of journalistic exemption.

1. How Section 44(3) will silence investigative journalism and whistleblowing

The RTI Act has enabled ordinary citizens, journalists, and activists to expose corruption that would otherwise remain hidden.[247] Activists and journalists used information often obtained through RTI or related disclosures to expose entrenched corruption in public works, environmental regulation, natural resource extraction, public recruitment, and welfare schemes.

Section 44(3) amends the RTI Act by modifying the exemption granted to personal information.[248] Under the earlier law, Section 8(1)(j) of the RTI Act,[249] allowed public authorities to withhold "personal information" only if it has no relationship to any public activity or interest, or if its disclosure would cause an unwarranted invasion of privacy. Notwithstanding these conditions, such personal information could be disclosed if "the larger public interest justified the disclosure."[250] This public-interest override provided journalists, activists, and citizens a critical tool to demand transparency when exposing corruption, maladministration, or other wrongdoing.[251]

The DPDP amendment removes that safeguard. Section 44(3) now mandates that any information classified as "personal information" cannot be disclosed under RTI, regardless of the public interest involved. This change completely eviscerates citizens' right to information. By making "personal information" off-limits, the amendment enables authorities to withhold documents that contain names, contact details, addresses, or other identifiers, even when such information is necessary to reveal patterns of corruption or misuse of public funds. In short, the amendment transforms the RTI from a transparency law into a law of denial.

The Supreme Court affirmed this in *K.S. Puttaswamy I*,[252] where the Court held that privacy and transparency must be balanced through proportionality. Any restriction on either right must be justified, necessary, and the least restrictive measure. This ensures that neither privacy nor transparency is reduced to a mere paper right.

---

[247] "RTI at 20: How RTI Exposed Corruption and Why the Govt Fears It | Jaanne Bhi Do Yaaro" (The Wire, 1 November 2025) https://www.thewire.in/government/rti-at-20-how-rti-exposed-corruption-and-why-the-govt-fears-it-jaanne-bhi-do-yaaro accessed 06 December 2025.
[248] DPDP Act, s. 44(3).
[249] Right to Information Act 2005, s. 8(1)(j).
[250] *Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi,* (2012) 13 SCC 61, p. 22, 23
[251] *R.K. Jain vs. Union of India,* (1993) 4 SCC 120, p. 54, 55
[252] *K.S. Puttaswamy I.*

In India, constitutional courts have time and again observed this balancing approach under Section 8(1)(j) of the RTI Act.[253] That provision protected personal information but permitted disclosure when a larger public interest required it. Courts repeatedly held that privacy must yield where disclosure serves accountability. In *Surupsingh Hrya Naik v. State of Maharashtra*,[254] the Bombay High Court considered whether the medical records of a legislator convicted of contempt could be withheld as "personal information." The Court held that the Indian Medical Council's confidentiality regulations[255] could not override the RTI Act,[256] and that personal information could be disclosed unless the third party made out a strong case for refusal. The Court also emphasised that the proviso to Section 8(1)(j) covers Parliament and State Legislatures with plenary powers, meaning that a wide range of information could be disclosed in public interest. Similarly, in *Vijay Prakash v. Union of India*, (2010),[257] the Delhi High Court held that privacy cannot defeat legitimate claims of public accountability. Even the Supreme Court's decision in *Girish Ramchandra Deshpande v. Central Information Commissioner*,[258] often cited to deny disclosure recognises that information may be released if a public interest is shown. Through this observation, the Court preserved the principle that transparency cannot be extinguished, even when the judiciary adopts heightened protection for individual privacy.

Section 44(3) of the DPDP Act allows public authorities to deny all requests containing "personal information" without considering public interest. Corruption investigations often rely on personnel records, financial disclosures, inspection notes, file notings, sanction orders, and correspondence all of which contain some form of personal information.[259] Even well-founded requests can be rejected on the ground that the relevant records contain "personal information", thereby withholding crucial evidence simply because it names individuals. This undermines accountability and weakens the public's ability to audit state actions. Pre-DPDP this information was disclosable if the public interest outweighed privacy. Courts in *Surupsingh Hrya Naik*, *Vijay Prakash*, and *Girish Ramchandra Deshpande* affirmed this principle. Section 44(3) of the DPDP Act overrides this safeguard and creates an absolute bar. Combined with the broad government exemptions under Section 17, this amendment creates a regime where opacity is the rule and transparency is the exception. This is why Section 44(3) is not a privacy-enhancing reform. It is a structural threat to public accountability and a direct assault on democratic governance.

Lastly, it is important to note that the DPDP Act does not define "personal information" because it only defines "personal data" as data about an individual who is identifiable by or in relation to such data. Personal information need not necessarily be "data" that is available in digital form or

[253] Right to Information Act 2005, s. 8(1)(j).
[254] *Surupsingh Hrya Naik v. State of Maharashtra*, AIR 2007 Bom 121
[255] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002, r 7.14.
[256] Right to Information Act 2005.
[257] *Vijay Prakash v. Union of India*, AIR 2010 Delhi 7
[258] *Girish Ramchandra Deshpande v. Central Information Commissioner*, 2012 AIR SCW 5865, p. 13
[259] United Nations Office on Drugs and Crime, Practical Guide on the Investigation of Corruption Cases (United Nations 2024).

non-digital form that is subsequently digitised, it can also be personal information collected by various public authorities that are non-digitised. RTI requests can be fulfilled by sending photocopies of non-digitised information, but according to the new amendment non-digitised personal information need not be disclosed.

2. Lack of a Journalistic Exemption and its Consequences

Unlike many data-protection regimes worldwide,[260] the DPDP Act does not include any carve-out for journalism or journalistic purposes. There is no provision that protects investigative reporters, whistle-blowers, or media organisations when they collect or process personal data for stories of public interest.

The lack of a journalistic exemption has at least two main consequences. First, a journalist or activist who collects names, addresses, contact details, or other personal information may qualify as a "Data Fiduciary" under the DPDP Act and become subject to all obligations of a Data Fiduciary. If they fail to obtain consent from each data subject, they may be liable for breach of the DPDP Act. This will chill investigative journalism and force journalists to self-censor to avoid massive penalties. Second, the DPDP Act allows imposition of fines up to Rs. 250 crore for non-compliance. This risk of heavy liability will discourage journalists and activists from handling or publishing any personal data, even when public-interest reporting demands it. As a result, individuals with power will evade scrutiny simply by labelling relevant information as "personal information".

Moreover, the legal definition of a "working journalist" under the Working Journalists and other Newspaper Employees (Conditions of Service) and Miscellaneous Provisions Act, 1955 mainly exists to set standards for pay, pensions and conditions for working journalists, rather than professional identification. This definition states that a "working journalist" means a person whose principal vocation is that of a journalist and who is employed either full- time or part-time in any newspaper establishment.[261] This includes an editor, a leader writer, news editor, sub-editor, feature-writer, copy-tester, reporter, correspondent, cartoonist, news-photographer and proof-reader, but does not include any such person who is employed mainly in a managerial, administrative, or supervisory capacity. This definition is primarily media-based (i.e. newspaper establishment) rather than a functional definition of journalists. However, in the context of applying a journalistic exemption to "journalists", it is not for the Central Government to decide who is and is not a journalist. Exemptions from onerous laws like data protection law should be granted based on the activity's function (journalistic activity or purpose), and not the identity or professional status of the journalist. This is particularly important today, as the nature of

[260] General Data Protection Regulation (EU) 2016/679, art 85; Data Protection Act, 2018 [UK], Part 5, Schedule II.

[261] Working Journalists and other Newspaper Employees (Conditions of Service) and Miscellaneous Provisions Act, 1955, s. 2(f).

journalism as an activity and profession is radically transforming. The rise of the blogger and user-based journalism has become immensely popular among both new and old media companies, a change that has drastically altered the definition of a journalist. Recognizing this, the Court of Justice of the European Union and the European Court of Human Rights, have noted that "journalistic purpose" exemption extends to anyone processing personal data for the sole purpose of disclosing information, opinions, or comments to the public.[262] The GDPR does not define "journalist" and this has allowed the European Court of Human Rights a broad purview to expand the exemption given to journalistic purposes. In the event the DPDP framework provided a legally circumscribed definition for a 'journalist' based on particular forms of media or functions, the exhaustive nature of definitions can limit the potential for more forms of journalistic activity to benefit from the exemption under a data protection law.

XI. THE DATA PROTECTION BOARD

The Data Protection Board ("**DPB/Board**") is the central body that is tasked with enforcing the DPDP Act. Notably, the DPB can be distinguished from other central regulatory bodies such as the Securities and Exchange Board of India (SEBI) or the Telecom Regulatory Body of India (TRAI) as it is a quasi-judicial body that is primarily responsible for the implementation of the law, grievance redressal, and the enforcement of penalties.

1. Establishment and Selection of the Board

The DPDP Act establishes the DPB, the quasi-judicial adjudicatory body responsible for the enforcement of the DPDP framework in India.[263] On 13 November 2025, the Central Government notified that the DPB will comprise four members.[264] The DPDP Act provides that the Chairperson and other Members of the DPB shall be individuals who possesses special knowledge or practical experience *inter alia* in the fields of data governance, information and communication technology, digital economy, regulation or techno-regulation, with at least one member of the DPB being an expert in the field of law.[265]

Under Rules 17(1) and 17(2), officials of the Central government are tasked with the constitution of a Search-cum-Selection Committees to recommend individuals for appointment as Chairperson and as members to the DPB.[266] Thus, under the present legal framework, ultimately,

---

[262] *Sergejs Buivids v. Datu valsts inspekcija,* Case C–345/17, 14 February 2019, available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=781330DFB5133FC37432F5CB0FEAC074?text=&docid=210766&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=605068; *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, 27 June 2017, available at: https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-175121%22%5D%7D.

[263] DPDP Act, s. 18(1).

[264] G.S.R. 845(E), Ministry of Electronics and Information Technology, November 13, 2025, [F. No. AA-11038/1/2025-CL&ES].

[265] DPDP Act, s.19(3).

[266] DPDP Rules, rules 17(1), 17(2).

the authority to finalise the appointments to the DPB rests with the Union government. This has raised concerns of executive control and questions regarding the independence and impartiality of the DPB.

2. Concerns regarding Executive influence over the Board

Given that the State, its agencies and the public sector itself are the largest data fiduciaries and processors, the Board's appointments process raises a reasonable apprehension regarding the independence of the Board, as the process could be influenced by political considerations, undermining the Board's credibility and impartiality. We have previously highlighted these concerns in IFF's submission on the Draft Digital Personal Data Protection Rules, 2025.[267] In our submission we observed that as the largest data fiduciary and processor of personal data is the public sector, the structure of the Board raises a justified, reasonable apprehension about the Board's independence, given that the process could be influenced by political considerations, which could in turn, undermine the Board's credibility and impartiality.[268]

The PDPB, 2019 which was an earlier version of the DPDP Act, originally recommended that the Selection Committee of the Data Protection Authority of India (DPA) (as it was referred to at the time) shall consist solely of executive members (a Cabinet Secretary as the chairperson and a secretary dealing with legal affairs and a secretary dealing with the Electronics and Information Technology as members).[269] The JPC Report noted that the proposed composition of the Selection Committee under the PDPB, 2019 had only three Members who were all bureaucrats at the level of Secretary and stated that it wished for the inclusion of technical, legal and academic experts in the Selection Committee in order to make it more "*inclusive, robust and independent*".[270] In that regard, the JPC Report proposed, *inter alia*, the inclusion of the Attorney General of India as a member and the inclusion of an independent expert from the fields of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or related subjects nominated by the Central government.[271] These recommendations were proposed keeping in mind the independence of the DPA.

The Supreme Court of India has consistently emphasised the need for tribunals in India to be independent from executive influence and has held that allowing the Central Government to appoint tribunal members is in violation of the independence of the judiciary.[272]

---

[267] The Internet Freedom Foundation, Detailed Submission on Behalf of the Internet Freedom Foundation to the Draft Digital Personal Data Protection Rules", March 4, 2025, available at: https://drive.google.com/file/d/11Kb8O10spvbR_vC5j1-uzwHYEpM0e2or/view?usp=sharing.
[268] ibid.
[269] Personal Data Protection Bill, 2019, s. 42(2).
[270] JPC Report, p. 128, clause 2.191.
[271] ibid., at p. 128, clause 2.191.
[272] *Madras Bar Association v. Union of India & Anr.*, AIR 2015 SC 1571.

In *Union of India v. R. Gandhi, President, Madras Bar Association* (2010) (MBA-I), the Supreme Court examined the constitutional validity of certain provisions of the Companies Act, 1956.[273] In MBA-I, the SC observed that tribunals could discharge judicial functions only if judicial independence was an assured guarantee, for which it was essential that Tribunal members not be bureaucrats.[274] The Supreme Court while considering recommendations for the better working of tribunals observed that, "*[o]nly if continued judicial independence is assured, Tribunals can discharge judicial functions. In order to make such independence a reality, it is fundamental that the members of the Tribunal shall be independent persons, not civil servants. They should resemble courts and not bureaucratic Boards. Even the dependence of Tribunals on the sponsoring or parent department for infrastructural facilities or personnel may undermine the independence of the Tribunal"*.[275]

The Court highlighted the gradual erosion of the independence of the judiciary, and the diminishing of the judiciary's space accompanied with the steady rise in the number of civil servants discharging functions as well as a gradual dilution of the standards and qualification.[276] In its recent judgement on tribunals,[277] the Supreme Court noted that MBA-I had previously highlighted that tribunals in India would continue being "*quasi-executive rather than quasi-judicial bodies*" without significant overarching reforms being undertaken that would structurally ensure the tribunal's independence in appointments, funding, and administration.[278] Thus, in MBA-I, the Supreme Court cautioned that tribunals cannot truly achieve their constitutional purpose without first being institutionally independent.[279]

In *Rojer Matthew v. South Indian Bank Ltd. & Ors.* (2019), the Supreme Court affirmed that there was a compulsory requirement to eliminate executive control over quasi-judicial bodies which discharged functions and responsibilities similar to the courts.[280] The Supreme Court noted that there is a compulsory need for exclusion of control of the Executive over quasi-judicial bodies of Tribunals discharging responsibilities akin to Courts. The Search-cum-Selection Committees as envisaged in Rule 17 of the DPDP Rules is against the constitutional scheme in as much as it dilutes the involvement of judiciary in the process of appointment of members of tribunals which is in effect an encroachment by the executive on the judiciary.

The Court further held that the principle of independence of the judiciary/the tribunal is a two-fold concept comprising: (i) independence of an individual judge, i.e. decisional independence; and (ii) independence of the judiciary or the tribunal as an institution or an organ

[273] 2025 SCC OnLine SC 2498.
[274] *Union of India v. R. Gandhi, President, Madras Bar Association,* (2010) 11 SCC 1.
[275] ibid, [20].
[276] ibid, [112].
[277] *Madras Bar Assn. v. Union of India,* 2025 SCC OnLine SC 2498 [33].
[278] *Madras Bar Association v. Union of India & Anr.*, 2025 SCC OnLine SC 2498, [33].
[279] *Madras Bar Association v. Union of India & Anr.*, 2025 SCC OnLine SC 2498, [33].
[280] *Rojer Mathew v. South Indian Bank Ltd.*, (2020) 6 SCC 1, [158].

of the State, i.e., functional independence. Functional independence would *inter alia* include the method of selection and qualifications prescribed, protection from interference and independence from the executive pressure, freedom from prejudices etc.

In *Madras Bar Association v. Union of India* (2025), the Supreme Court held that a tribunal system designed by Parliament must be consistent with values that are constitutional prerequisites such as independence, impartiality, and effective adjudication.[281] The Supreme Court further noted that, "*[a] law that undermines these foundational values, such as by enabling executive control over appointments, curtailing tenure arbitrarily, or weakening institutional autonomy, does not merely offend an "abstract principle". It strikes at the core of the constitutional arrangement.*"[282]

3. Functions and Powers of the DPB

Section 27 of the DPDP Act provides for the powers and functions of the DPB, which can broadly be categorized as powers related to conducting an inquiry i.e. investigative powers, and powers to issue directions.[283] As per Section 27(1)(a) of the DPDP Act, the DPB is empowered to direct any urgent remedial or mitigation measures in the event of a personal data breach, and inquire into and impose penalties on such a breach.[284]

The circumstances in which the DPB is empowered to inquire into a personal data breach and impose a penalty, are namely:[285]

1. on a complaint made by a Data Principal regarding a personal data breach;
2. on a breach by a Data Fiduciary in observance of its obligations in relation to the Data Principal's personal data or the exercise of their rights under the DPDP Act. Under Section 8(6) of the DPDP Act, the Data Fiduciary shall give the DPB *and* each Data Principal who has been affected, intimation of any personal data breach;
3. on a reference made to the DPB by the Central Government or by a State Government;
4. in compliance with the directions of any court;
5. on a complaint made by a Data Principal regarding a breach of obligations related to the Data Principal's personal data by a Consent Manager;
6. on receipt of an intimation of breach of any condition of registration of a Consent Manager; and
7. on a reference made by the Central Government regarding a breach in observance of Section 37(2) by an intermediary. Section 37(2) of the DPDP Act provides that every

[281] 2025 SCC OnLine SC 2498.
[282] *Madras Bar Assn. v. Union of India, 2025 SCC OnLine SC 2498,* [126].
[283] DPDP Act, s. 27.
[284] DPDP Act, s. 27(1)(a).
[285] DPDP Act, s.27(1).

intermediary who receives a direction from the Central Government shall be bound to comply with such a direction.

Further, under Section 27(2) of the DPDP Act, the DPB has the authority to issue directions after hearing the concerned person and recording its reasons in writing, which will be binding.[286] The DPB is empowered to modify, suspend, withdraw, or cancel such directions and impose the conditions necessary to do so, if a representation is made to the DPB either by a person affected by the direction *or* on a reference made by the Central Government.[287]

4. Procedure of the DPB

4.1. DPB vested with Powers of a Civil Court

The DPB is vested with the same powers as a civil court under the Code of Civil Procedure, 1908 for discharging its functions under the DPDP Act.[288] These powers include:

a. summoning and enforcing the attendance of any person;
b. examining any such person under oath;
c. receiving evidence requiring the discovery and production of documents;
d. inspecting any data, book, document, register, books of account or any other document; and
e. such other matters as may be prescribed.

4.2. Power of the DPB to Conduct an Inquiry

Upon receiving an intimation, complaint, reference or direction under Section 27(1) of the DPDP Act,[289] the DPB can proceed with:[290]

a. determining whether there are sufficient grounds to proceed with an inquiry,
b. determining whether there are sufficient grounds to proceed with an inquiry,
c. close the proceedings (by recording reasons in writing) upon determining that there are insufficient grounds for an inquiry.

In a situation where the DPB determines that there are sufficient grounds to proceed with an inquiry, after recording its reasons in writing, the DPB is empowered to inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the DPDP Act.[291] The DPB is expected to follow the principles of natural justice and record reasons

[286] DPDP Act, s.27(2).
[287] DPDP Act, s. 27(3).
[288] DPDP Act, s. 28(7).
[289] DPDP Act, s. 27(1).
[290] DPDP Act, s. 28(2).
[291] DPDP Act, s. 28(5).

for its actions while conducting an inquiry.[292] Further, the DPB is empowered to issue interim orders during the course of the inquiry, as it deems necessary after giving the concerned person an opportunity of being heard. On completion of the inquiry and after giving the person concerned an opportunity of being heard, the DPB may either close the proceedings or proceed in accordance with Section 33 (Penalties), with reasons for the decision recorded in writing.

4.3. Ancillary Powers of the DPB

If the DPB may need the services of any police officer or any officer of the Central Government or a State Government to assist it and it shall be the duty of every such officer to comply with such requisition.[293] At any stage after receipt of a complaint, if the DPB is of the opinion that the complaint is false or frivolous, it is empowered to issue a warning or impose costs on the complainant.[294]

4.4. Safeguards against Powers of the DPB

A noteworthy procedural safeguard is provided in Section 28(8) of the DPDP Act which states that the DPB or its officers shall not prevent access to any premises or take into custody any equipment or item that may "adversely affect" the day-to-day functioning of a person.[295]

4.5. Appeal

An appeal against an order or direction of the DPB lies before an appellate tribunal which is the Telecom Disputes Settlement and Appellate Tribunal.[296] The Appellate Tribunal is not bound by the procedure laid down by the Code of Civil Procedure, 1908, but by the principles of natural justice and is empowered to regulate its own procedure.[297]

4.6. Penalties

If the DPB concludes that a breach is significant, it is empowered to impose monetary penalties as specified in the DPDP Act's Schedule.[298] The DPB shall consider the following factors while determining the amount of monetary penalty to be imposed:

a. the nature, gravity and duration of the breach;
b. the type and nature of the personal data affected by the breach;

[292] DPDP Act, s. 28(6).
[293] DPDP Act, s. 28(9).
[294] DPDP Act, s. 28(12).
[295] DPDP Act, s. 28(8).
[296] DPDP Act, s. 2(a).
[297] DPDP Rules, rule 22(3)(a).
[298] DPDP Act, s. 33(1).

c. repetitive nature of the breach;
d. whether the person, as a result of the breach, has realised a gain or avoided any loss;
e. Any action taken by the person to mitigate the effects and consequences of the breach, the timeliness and effectiveness of such action;
f. whether the monetary penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the DPDP Act; and
g. the likely impact of the imposition of the monetary penalty on the person.

Besides breach in observance of the duties of Data Principals,[299] all other breaches of any of the provisions of the DPDP Act attract penalties which may extend to crores of rupees, irrespective of the capacity of the Data Fiduciary. The highest penalty among these is for breach of reasonable security safeguards to prevent personal data breach, which may attract up to Rupees 250 crores of penalty.[300]

THE SCHEDULE

[*See* section 33 (*1*)]

Sl. No.	Breach of provisions of this Act or rules made thereunder	Penalty
(1)	(2)	(3)
1.	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (*5*) of section 8.	May extend to two hundred and fifty crore rupees.
2.	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (*6*) of section 8.	May extend to two hundred crore rupees.
3.	Breach in observance of additional obligations in relation to children under section 9.	May extend to two hundred crore rupees.
4.	Breach in observance of additional obligations of Significant Data Fiduciary under section 10.	May extend to one hundred and fifty crore rupees.
5.	Breach in observance of the duties under section 15.	May extend to ten thousand rupees.
6.	Breach of any term of voluntary undertaking accepted by the Board under section 32.	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted.
7.	Breach of any other provision of this Act or the rules made thereunder.	May extend to fifty crore rupees.

[299] DPDP Act, Schedule, item 5.
[300] DPDP Act, Schedule, item 1.

INTERNET
FREEDOM
FOUNDATION

policy@internetfreedom.in