

**IN THE HON'BLE SUPREME COURT OF INDIA**  
**WRIT PETITION (C) NO. \_\_\_\_\_/2026**  
**PUBLIC INTEREST LITIGATION**  
**UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA**

**IN THE MATTER OF:**

**VENKATESH NAYAK** **...PETITIONER**

**VERSUS**

**UNION OF INDIA** **...RESPONDENT**

**WITH**

**I.A. NO. \_\_\_\_\_/2026: APPLICATION FOR DIRECTIONS**

**PAPERBOOK**

**(FOR INDEX: KINDLY SEE INSIDE)**

**ADVOCATE FOR PETITIONER: AAKARSH KAMRA**

**FILED ON: 06.02.2026**

## INDEX

Sl. No.	Particulars of Documents	Page No. of Part to which it belongs		Remarks
		Part I (Contents of Paper Book)	Part II (Contents of file alone)	
(i)	(ii)	(iii)	(iv)	(v)
1.	Court Fees			
2.	Listing Proforma	A1- A2	A1- A2	
3.	Cover Page of Paper Book	A3	A3	
4.	Index of Record of Proceedings	A4	A4	
5.	Limitation Report Prepared by Registry	A5	A5	
6.	Defect List	A6	A6	
7.	Note Sheet		NS 1 to	
8.	Synopsis & List of Dates	B-G		
9.	Writ Petition with Affidavit	1-35		
10.	<b><u>Annexure P1</u></b> : A true and correct copy of the Digital Personal	36-56		

	Data Protection Act 2023			
11.	<b>Annexure P2:</b> True Copy of GSR 843(E) dated 13.11.2025	57-58		
12.	<b>Annexure P3:</b> True and correct copy of the Digital Personal Data Protection Rules 2025.	59-76		
13.	IA NO _____ OF 2026: Application for Directions	77-80		
14.	Filing Index		81	
15.	Vakalatnama and Memo of Appearance with PAN card and Aadhar Card of the Petitioner.		82-84	

**FILED ON: 06.02.2026**

PROFORMA FOR FIRST LISTING

SECTION \_\_\_\_\_

The case pertains to (Please tick/check the correct box):

- Central Act: (Title) CONSTITUTION OF INDIA
- Section: 14,19 AND 21
- Central Rule: (Title) DIGITAL PERSONAL DATA PROTECTION RULES 2025
- Rule No(s) NA
- State Act: (Title) NA
- Section: NA
- State Rule: (Title) NA
- Rule No(s) NA
- Impugned Interim Order: (Date) NA
- Impugned Final Order/Decree: (Date) NA
- High Court: (Name) NA
- Names of Judges: NA
- Tribunal/Authority: (Name) NA
1. Nature of matter:  Civil  Criminal
2. (a) Petitioner/appellant No. 1: VENKATESH NAYAK  
(b) e-mail ID: [REDACTED]  
(c) Mobile phone number: NA
3. (a) Respondent No. 1: UNION OF INDIA  
(b) e-mail ID: NA  
(c) Mobile phone number: NA

4. (a) Main category classification: 27P  
(b) Sub classification: 2702
5. Not to be listed before: NA
6. (a) Similar disposed of matter with citation, if any, & case details: NO SIMILAR MATER HAS BEEN DISPOSED OFF  
(b) Similar pending matter with case details: NO SIMILAR MATTER IS PENDING
7. Criminal Matters: NOT A CRIMINAL CASE  
(a) Whether accused/convict has surrendered:  Yes  No  
(b) FIR No. NA Date: NA  
(c) Police Station: NA  
(d) Sentence Awarded: NO  
(e) Period of sentence undergone including period of detention/custody undergone NO  
(f) **Whether any earlier case between the same parties is filed** NO  
(g) **Particulars of the FIR and Case** NO  
(h) **Whether any bail application was preferred earlier and decision thereupon** NO
8. Land Acquisition Matters:  
(a) Date of Section 4 notification: NA  
(b) Date of Section 6 notification NA  
(c) Date of Section 17 notification NA
9. Tax Matters: State the tax effect: NA
10. Special Category (first petitioner/appellant only): NA  
 Senior Citizen > 65 years  SC/ST  Woman/Child  Disabled  
 Legal aid case  In custody
11. Vehicle Number (in case of Motor Accident Claim matters): NA
12. **Whether there was / is litigation on the same point of law, if yes, details thereof** NO

Date: 06.02.2026

AOR for petitioner(s)/appellants(s)  
(Name) AAKARSH KAMRA  
Registration No. 2599



## SYNOPSIS AND LIST OF DATES AND EVENTS

The Petitioner has approached this Hon'ble Court by filing the present petition in public interest under Article 32 of the Constitution of India, seeking *inter-alia*, that this Hon'ble Court may be pleased to declare that Sec. 44(3) and Secs. 17(1)(c), 17(2), 33(1), 36 of The Digital Personal Data Protection Act, 2023, (hereinafter referred to as "DPDP Act") as well as Rules 17 and 23(2) of The Digital Personal Data Protection Rules, 2025, are *ultra vires* the Constitution, and other consequential reliefs.

### **Right to Information and Right to Know - Fundamental Rights under Articles 19(1)(a) and 21 of the Constitution**

The right to information and right to know of citizens is part of the rights and freedoms guaranteed under Articles 19(1)(a) and 21 of the Constitution of India. This has been held in various judgments of this Hon'ble Court including *PUCL vs Union of India* (2003) 4 SCC 399, *Union of India v. Association for Democratic Reforms*, (2002) 5 SCC 294 and *Reliance Petrochemicals vs Proprietors of Indian Express Newspapers* (1988) 4 SCC 592.

In furtherance of the fundamental right to information, Parliament had enacted the Right to Information Act, 2005 (hereinafter referred to as "RTI Act"). The constitutional principle and norm with regard to public functionaries and public duties is that information must be shared in the interest of transparency ensuring open governance. Parliament while enacting the RTI Act, in Section 4(1)(b) provided for mandatory voluntary disclosures to be made by public authorities to give effect to the citizens' right to information and right to know. The RTI Act, in Section 8(1), carves out a narrow and limited scope for exemptions to the disclosure of information, and unless the information sought

is specifically covered under an exception, publishing the information is statutorily mandatory. Further, the onus to justify the denial of a request for information is also on the Public Information Officer, and the reason for a citizen seeking information is not open to scrutiny under the RTI Act.

### **The Digital Personal Data Protection Act, 2023, and the amendment to Section 8(1)(j) of the Right to Information Act, 2005**

The Digital Personal Data Protection Act, 2023, brought into operation vide GSR 843(E) on 13.11.2025, through Section 44(3) amended Section 8(1)(j) of The Right to Information Act, 2005. Section 44(3) of DPDP Act provides that in Section 8(1) of the RTI Act, for existing clause (j), the following clause shall be substituted: “(j) *information which relates to personal information;*”. A comparative table of Section 8(1)(j) of RTI Act before and after the amendment is produced below for reference:

<b>Unamended Clause</b>	<b>Amended Clause</b>
<p data-bbox="443 1160 863 1294">8. <i>Exemption from disclosure of information.—</i></p> <p data-bbox="443 1355 863 1590">(1) <i>Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—</i></p> <p data-bbox="443 1653 863 1982">(j) <i>“information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause</i></p>	<p data-bbox="981 1171 1401 1305">8. <i>Exemption from disclosure of information.—</i></p> <p data-bbox="981 1366 1401 1601">(1) <i>Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—</i></p> <p data-bbox="981 1664 1401 1798">(j) <i>“information which relates to personal information;”</i></p>

<p><i>unwarranted invasion of the privacy of the individual, unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:</i></p> <p><i>Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.”</i></p>	
---	--

The Petitioner submits that vide the above amendment, Section 8(1)(j) of RTI Act has been stripped of the three pronged test that it originally contained and now operates as a blanket ban on the obligation to disclose personal information. Earlier, prior to the amendment, the Public Information Officer or First Appellate Authority was statutorily equipped and required to carry out a three pronged test as detailed below under Section 8(1)(j):

- i. Test of public activity
- ii. Test of unwarranted invasion
- iii. Mandatory public interest override to facilitate disclosure

The Petitioner submits that a blanket bar on the obligation to disclose all personal information, without the statutory scheme to balance it against larger

public interest, renders Section 44(3) of DPDP Act liable to be struck down on multiple counts, including *inter-alia*:

- a) It is an unreasonable restriction on the right under Article 19(1)(a); and
- b) Privacy is not a fundamental right available to the State; and
- c) Privacy is not a ground for restriction under Article 19(2); and
- d) It fails the 5 pronged proportionality test; and
- e) It violates Article 14 by equating privacy of public functionaries to that of ordinary citizens; and
- f) It inverts the jurisprudence of privacy viz-a-viz the right to information; and
- g) It prioritizes privacy over the larger public interest of transparency and open governance, which is unconstitutional and against the dicta of *PUCL vs Union of India* (2003) 4 SCC 399, as reiterated in *KS Puttaswamy vs Union of India* (2019) 1 SCC 1.
- h) It accords unguided discretion to the executive to deny personal information, which is unconstitutional.

The Petitioner submits that the amendment to Section 8(1)(j) of the RTI Act, when read in conjunction with the definition of the term “personal data” in Section 2(t) read with Section 3(a)(ii) of the DPDP Act, brings within its fold all information which even remotely relates to the identity of an individual, and renders the right to information illusory. It allows the executive to deny information to citizens by citing the personal nature of the information, even for public functionaries entrusted with public duties. It is a death knell for participatory democracy, and ruinous to ideas of open governance, which must guide the Indian polity in consonance with the Constitutionally recognized fundamental right of the citizen to know and be informed.

Rules 17(1) and (2) of the DPDP Rules provide for constitution of Search-cum-Selection Committees for appointment of the Chairperson and

other members of the Board, and executive dominance in the formation of the said Committee is violative of the doctrine of separation of powers, given that the Board performs quasi judicial functions.

Further, the Petitioner submits that Sections 17(1)(c), 17(2), 33(1) and 36 of the DPDP Act, as well as Rule 23(2) of the DPDP Rules, which have been notified by GSR 843(E) and GSR 846(E) dated 13.11.2025, but will come into force eighteen months after the notification, are also unconstitutional and violate Articles 14, 19(1)(a) and 21 of the Constitution.

Sections 17(1)(c) and 17(2), insofar as they exempt application of provisions of the DPDP Act either in part or whole, facilitate the operation of a surveillance regime with no necessary safeguards or review mechanism, thereby failing the necessary safeguards prong of the proportionality test. Section 36, in a similar vein, allows the Central Government to call for any information without any statutory guidance or limitation on the scope and reasons for calling such information from the Data Board of Data Fiduciaries. This makes the provision fall foul of the test of manifest arbitrariness as it violates Article 14.

Section 33(1), in providing penalties for data breach, states that penalties shall be imposed when after inquiry the Data Board concludes that the data breach is “significant”, without any statutory guidance as to what constitutes a “significant” data breach. Unbridled discretion in that regard brings the provision within the vice of arbitrariness and violates Article 14.

Thus, in view of the immediate effect given to Section 44(3) of the DPDP Act and Rule 17 of the DPDP Rules, as well as the impending commencement of other unconstitutional provisions in the said Act and Rules, the Petitioner is constrained to file the present petition in public interest seeking declaratory reliefs to protect and further the fundamental right of citizens to information; the right to know; the right of participatory democracy as a facet of the right to life; and to ensure that two decades of transparency in the life of public authorities is

not reversed into an era of dark opacity, on a fallacious legislative attempt to uphold the right to privacy.

### **LIST OF DATES AND EVENTS**

<b>DATES</b>	<b>EVENTS</b>
15.06.2005	The Right to Information Act, 2005, received Presidential assent.
11.08.2023	The Digital Personal Data Protection Act, 2023, received the assent of the President of India.
13.11.2025	The Digital Personal Data Protection Rules, 2025, were published in the Official Gazette vide GSR 846(E), and on the same day GSR 843(E) brought into commencement certain parts of The Digital Personal Data Protection Act, 2023, including Section 44(3) which amends Section 8(1)(j) of The Right to Information Act, 2005. Sections 17(1)(c), 17(2), 33(1) and 36 were also notified vide GSR 843(E) but the said provisions shall come into force eighteen months from the date of publication of GSR 843(E).
06.02.2026	Hence this petition in public interest.

IN THE HON'BLE SUPREME COURT OF INDIA

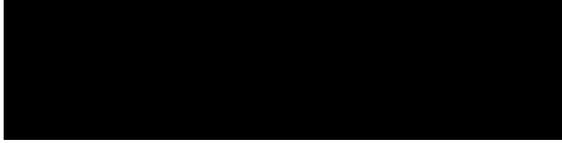
WRIT PETITION (C) NO. **177**/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA

IN THE MATTER OF:

**1.VENKATESH NAYAK**



**...PETITIONER**

**VERSUS**

**1. UNION OF INDIA**

Through The Secretary

Ministry of Law and Justice

4th Floor, A- Wing

Shastri Bhawan, New Delhi - 110001

**...RESPONDENT**

**WRIT PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA SEEKING A DECLARATION THAT SECTIONS 44(3), 17(1)(c), 17(2), 33(1), AND 36 OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, READ WITH THE SCHEDULE AND RULE 17 and 23(2) OF THE RULES MADE THEREUNDER ARE UNCONSTITUTIONAL FOR VIOLATING ARTICLES 14, 19(1)(a), AND 21 OF THE CONSTITUTION, AND OTHER CONSEQUENTIAL RELIEFS.**

TO,

THE HON'BLE CHIEF JUSTICE OF INDIA AND HIS  
COMPANION JUDGES OF THE HON'BLE SUPREME COURT  
OF INDIA

THE HUMBLE PETITION OF THE  
PETITIONER ABOVE-NAMED

**MOST RESPECTFULLY SHOWETH:**

1. That the Petitioner has approached this Hon'ble Court by filing the present petition in public interest under Article 32 of the Constitution of India, seeking *inter-alia*, that this Hon'ble Court may be pleased to declare that Secs. 17(1)(c), 17(2), 33(1), 36 and Sec. 44(3) of The Digital Personal Data Protection Act, 2023, (hereinafter referred to as "DPDP Act") as well as Rules 17 and 23(2) of The Digital Personal Data Protection Rules, 2025, are *ultra vires* the Constitution, and other consequential reliefs.

#### **1A. ABOUT THE PETITIONER**

The Petitioner Venkatesh Nayak has authored public education documents on,, issues of social justice, electoral reforms, efficacy of public audit mechanisms, and citizens' right to information. He was closely associated with the process of advocacy for the Right to Information Act, 2005.

The Petitioner being an expert on the issue has designed and conducted training programmes for implementing the RTI Act 2005 for senior and middle level officers of government serving in Uttarakhand, Madhya Pradesh, Gujarat, Meghalaya, Nagaland, Tripura, Mizoram, Delhi, Tamil Nadu, Jharkhand, Bihar, Uttar Pradesh, Punjab Haryana and West Bengal. He has been a workshop designer and resource person at training workshops organised by the Institute of Secretariat Training and Management, Delhi for Public Information Officers (PIOs) and RTI Trainers designated by the Government of India. He has been invited by the National Institute of Administration and Research of the Lal Bahadur Shastri National Academy of Administration, Mussoorie, National Academy of Customs, Indirect Taxes and Narcotics, the Pandit Deen Dayal National Academy of Social Security, the Institute of Government Accounts and Finances, the National Academy of Direct Taxes, the Postal Staff College, Dr. R. S. Tolia Uttarakhand Academy of Administration and the Meghalaya Administrative Training Institute as a resource person for training PIOs and senior government officers. Till date he has sensitised and trained more than 8,300 government officers in various jurisdictions.

The Petitioner was a member of the Sub-Committee appointed by the Policy Advisory group of SCOPE (Standing Conference of Public Enterprises) to advise Public Sector Undertakings (PSUs) for implementing the RTI Act. He has been a resource person at in-house training workshops organized by PSUs such as the Food Corporation of India, the National Buildings Construction Corporation of India, the Power Grid Corporation of India, the Oriental Insurance Company Ltd., and other agencies like the Punjab State Electricity Board, the West Bengal State Electricity Board, the Employees State Insurance Corporation Ltd., Housing and Urban Development Corporation (HUDCO), Steel Authority of India (SAIL), Airports Authority of India and the National Capital Region Planning Board. Till date he has trained more than 800 executives and managers of various Central and State level Public Sector Enterprises for implementing the RTI Act. The Petitioner has provided technical support to governments and CSOs engaged in drafting or reforming RTI laws in Afghanistan, Bangladesh, Canada, Fiji, Ghana, Kenya, Malaysia, Malta, the Maldives, Sri Lanka, Tanzania and Zambia. He has designed and conducted capacity building workshops on RTI for Members

of Parliament, Information Commissioners, senior government officers, civil society and media representatives in Egypt, Ghana, Kenya, Liberia, Nigeria, Tanzania, Uganda and Zambia in Africa; Afghanistan, Bangladesh, Bhutan, Jordan, the Maldives, Nepal, Sri Lanka and Vietnam in Asia; Dominica in the Caribbean and Fiji in the Pacific. The Petitioner therefore has significant expertise in the field of constitutional jurisprudence and the statutory framework of the Right to Information Act, 2005.

**1B.** That in accordance with ORDER XXXVIII Rule 12 of the Supreme Court Rules, 2013, the Petitioner declares the following personal information:

a) Name: Venkatesh Nayak

b) Address:

c) Email address: [REDACTED]

d) PAN card No.:

e) Aadhaar No.:

f) Annual Income (Approx):

**1C.** That the Petitioner states that he has adequate means to bear the costs of litigation, as may arise.

**1D.** That the Petitioner has not filed any similar petition either before this Hon'ble Court or any other court or fora.

**1E.** That the Petitioner does not have any personal gain, private motive or oblique reason for filing of the present Public Interest Litigation.

**1F.** That there is no likely injury to result to any member of the public if the present petition is allowed.

**1G.** That the Petitioner has no personal interest in the subject matter of the Petition, and he is not involved in any litigation which could have a nexus or bearing on the outcome of this case or vice-versa. The Petitioner has filed the present petition solely in the interest of the general public seeking judicial review of the constitutionality of the imputed provisions.

## **BRIEF FACTS**

- 2.** That the right to information and right to know of citizens is part of the rights and freedoms guaranteed under Articles 19(1)(a) and 21 of the Constitution of India. In furtherance

of the fundamental right to information, Parliament had enacted the Right to Information Act, 2005 (hereinafter referred to as “RTI Act”). The constitutional principle and norm with regard to public functionaries and public duties is that information must be shared in the interest of transparency ensuring open governance. Parliament while enacting the RTI Act, in Section 4(1)(b) provided for mandatory voluntary disclosures to be made by public authorities to give effect to the citizens’ right to information and right to know. The RTI Act, in Section 8(1), carves out a narrow and limited scope for exemptions to the disclosure of information, and unless the information sought is specifically covered under an exception, publishing the information is statutorily mandatory. Further, the onus to justify the denial of a request for information is also on the Public Information Officer, and the reason for a citizen seeking information is not open to scrutiny under the RTI Act.

- 3.** The DPDP Act was notified on 11.08.2023, but it did not come into force immediately, as Section 1(2) of the Act requires a separate notification for commencement of the

Act. A true and correct copy of the Digital Personal Data Protection Act 2023 dated 11.08.2023 is being annexed herewith as **Annexure P1(At Pages\_36\_to\_56\_)**. By virtue of the commencement notification GSR 843(E) dated 13.11.2025, Section 44(3) came into force, which provided for substitution of Section 8(1)(j) of the RTI Act, 2005, by amendment. Section 44(3) of DPDP Act provides that in Section 8(1) of the RTI Act, for existing clause (j), the following clause shall be substituted:

*“(j) information which relates to personal information;”*

[True Copy of GSR 843(E) dated 13.11.2025 is annexed as **ANNEXURE P2 at Pages 57-58**].

[True and correct copy of the Digital Personal Data Protection Rules 2025 dated 13.11.2025 is being annexed herewith as **Annexure P3 at Pages 59-76**].

4. That in order to highlight the extensive change introduced through Section 44(3) of DPDP Act, a comparative table of Section 8(1)(j) of RTI Act before and after the amendment is produced below:

Unamended Clause	Amended Clause
<p data-bbox="491 327 911 461">8. <i>Exemption from disclosure of information.—</i></p> <p data-bbox="491 524 911 757">(1) <i>Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—</i></p> <p data-bbox="491 819 911 1742">(j) <i>“information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual, unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:</i></p> <p data-bbox="491 1756 911 1989"><i>Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be</i></p>	<p data-bbox="1029 338 1449 472">8. <i>Exemption from disclosure of information.—</i></p> <p data-bbox="1029 535 1449 768">(1) <i>Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—</i></p> <p data-bbox="1029 831 1449 965">(j) <i>“information which relates to personal information;”</i></p>

<i>denied to any person.”</i>	
-------------------------------	--

5. That vide the impugned amendment, Section 8(1)(j) of RTI Act has been stripped of the three pronged test that it originally contained and now operates as a blanket ban on the obligation to disclose personal information. Earlier, prior to the amendment, the Public Information Officer or First Appellate Authority was statutorily equipped and required to carry out a three pronged test as detailed below under Section 8(1)(j):

- Test of public activity
- Test of unwarranted invasion
- Mandatory public interest override to facilitate disclosure

6. In view of Section 44(3) of DPDP Act, a sweeping amendment to Section 8(1)(j) of RTI Act has been introduced which destroys the internal framework, operation and spirit of the RTI Act. It has inverted the law on transparency and open governance, which are facets of democracy which is constitutive of the basic structure of the Indian Constitution. Further, the DPDP Act commits a

constitutional fallacy in tracing the right to privacy to the State, and placing the right to privacy of State agents and public functionaries entrusted with public duties at par with ordinary citizens. It amounts to an unreasonable restriction and fails the proportionality test, as it interferes with the right to information which is a fundamental right under Articles 19(1)(a) and 21, while privacy is not a permissible restriction as it does not find mention in Article 19(2). In doing so, Section 44(3) of DPDP Act violates Sections 14, 19(1)(a) and 21 of the Constitution of India.

7. Further, Sections 17(1)(c), 17(2), 33(1) and 36 of the DPDP Act, as well as Rules 17 and 23(2) of the DPDP Rules, are also *ultra vires* the Constitution, for reasons detailed below in the Grounds.
8. In view of the above, the Petitioner has been constrained to file the present petition in public interest *inter-alia* on the following grounds, which may be read jointly and severally, and without prejudice to one another:

## 9. GROUNDS

**A. BECAUSE** Sec. 17(1)(c), 17(2), 33(1), 36 and Sec 44(3) of the DPDP Act, as well as Rules 17 and 23(2) are *ultra vires* the Constitution and liable to be struck down.

### **Right to Information and the Right to Know are Fundamental Rights**

**B. BECAUSE** the RTI Act, 2005, is a statutory embodiment of the fundamental right to know; the right to make informed choices; and an inalienable facet of the idea of representative democracy; which forms part of the basic structure of the Indian Constitution. The right to know was judicially recognized to emanate from Part III of the Constitution, decades prior to the enactment of the RTI Act, 2005. In *State of U.P. v. Raj Narain*, (1975) 4 SCC 428, this Hon'ble Court recognized that people have the right to know about public acts done by public functionaries. Similar observations emphasizing the principle that in regard to public functions, disclosure is the rule while secrecy is the exception, form the ratio of various judgments such as *S.P. Gupta v. Union of India*, 1981 Supp SCC 87, *Union of India v. Association for Democratic Reforms*, (2002) 5 SCC 294, and *People's Union for Civil Liberties v. Union of India*, (2003) 4 SCC 399.

**C. BECAUSE** this Hon'ble Court has also held that the right to know also traces its origin to Article 21, and is an inalienable facet of the right to life and the right to live in a participatory democracy. Reliance is placed herein on *Reliance Petrochemicals vs Proprietors of Indian Express Newspapers* (1988) 4 SCC 592, where this Hon'ble Court held,

*“We must remember that the people at large have a right to know in order to be able to take part in a participatory development in the industrial life and democracy. Right to Know is a basic right which citizens of a free country aspire in the broader horizon of the right to live in this age in our land under Article 21 of our Constitution. That right has reached new dimensions and urgency. That right puts greater responsibility upon those who take upon the responsibility to inform.” [Emphasis Supplied]*

**D. BECAUSE** provisions of the RTI Act, having been enacted in furtherance of ensuring guaranteed fundamental rights under Part III, cannot be curbed or curtailed through amendments introduced in the DPDP Act, 2023, that traverse into subject domain which is beyond the scope of the DPDP Act. This is particularly significant, as the said amendment in effect amends fundamental rights, by curtailing the scope of the fundamental right to know and right to information in the RTI Act, 2005. The Constitution Bench judgment in *CPIO, Supreme Court of India v. Subhash Chandra*

*Agarwal*, (2020) 5 SCC 481, reiterates and reaffirms that the right to know and the right to information are categorically borne out of the guarantees in Article 19(1)(a) of the Constitution. Thus, conflict between any part of the DPDP Act and that of pro-disclosure provision(s) of the RTI Act, is not a case of statutory conflict *simpliciter*. Rather it needs to be considered as statutory expansion under DPDP Act of curtailments/infringements to the fundamental right to know and right to information, which must satisfy the test of Article 19(2), as well as the test of reasonableness and the other five prongs of the doctrine of proportionality.

**E. BECAUSE** it is no longer *res integra* that fundamental rights recognized by the expansive jurisprudence developed by this Hon'ble Court about Part III of the Constitution cannot be treated as derivative rights and are equally enforceable as other fundamental rights explicitly mentioned in Part III of the Constitution, as held in *PUCL vs Union of India* (2003) 4 SCC 399.

**Privacy not a restriction under Article 19(2)**

**F. BECAUSE** once this Hon'ble Court has held that right to information is rooted *inter-alia* in Article 19(1)(a), the said right may be curtailed only by reasonable restrictions laid down in Article 19(2) of the Constitution. Pertinently, the right to privacy is

not one of the restrictions in Article 19(2), and the DPDP Act through the impugned amendment thus cannot curb the right to information and the right to know. Reliance is placed herein on *PUCL vs Union of India* (2003) 4 SCC 399, where this Hon'ble Court held that Section 33-B as introduced by The Representation of People (Third Amendment ) Act, 2002, was *ultra vires* the Constitution as it amounted to an unreasonable restriction on the right to know and could not be traced to any of the restrictions under Article 19(2). It was categorically held that legislative competence to pass law which interferes with the right to information under Article 19(1)(a) is limited as provided in Article 19(2).

**Public interest overrides right to privacy of public functionaries**

**G. BECAUSE** this Hon'ble Court when tasked with balancing the right to privacy against larger public interest, has always leaned towards the latter. The larger public interest of the citizens' right to information and right to know under Article 19(1)(a) and Article 21 cannot be thwarted by elevating individual right to privacy of public functionaries to an exalted position in the constitutional scheme. In *PUCL* (2003), this Hon'ble Court had held,

*“By calling upon the contesting candidate to disclose the assets and liabilities of his/her spouse, the fundamental right to information of a voter/citizen is thereby promoted. When there is a competition between the right to privacy of an individual and the right to information of the citizens, the former right has to be subordinated to the latter right as it serves the larger public interest. The right to know about the candidate who intends to become a public figure and a representative of the people would not be effective and real if only truncated information of the assets and liabilities is given. It cannot be denied that the family relationship and social order in our country is such that the husband and wife look to the properties held by them as belonging to the family for all practical purposes, though in the eye of law the properties may distinctly belong to each of them. By and large, there exists a sort of unity of interest in the properties held by spouses. The property being kept in the name of the spouse benami is not unknown in our country. In this situation, it could be said that a countervailing or paramount interest is involved in requiring a candidate who chooses to subject himself/herself to public gaze and scrutiny to furnish the details of assets and liabilities of the spouse as well.” [Emphasis Supplied]*

Pertinently, the above observations in *PUCL (2003)* have been reaffirmed by the Constitution Bench decision in *KS Puttaswamy vs Union of India (2019) 1 SCC 1*.

**H. BECAUSE** it is well settled that any act of Parliament which leads to a curtailment of the fundamental rights must be narrowly construed to pass muster as “least restrictive measure” under the proportionality test. Accordingly, Sec. 44(3) of DPDP Act cannot traverse into aspects and provisions of the RTI Act which govern

information other than “digital personal data”. Reliance is placed herein on *KS Puttaswamy vs Union of India* (2017) 10 SCC 1, *Ramesh Chandra Sharma vs State of Uttar Pradesh* (2024) 5 SCC 217 and other judgments of this Hon’ble Court which mandate judicial review of legislation curtailing fundamental rights by employing all five prongs of the ‘proportionality test’.

**Section 44(3) not limited to “digital personal data”, thus travels beyond the scope of the DPDP Act**

- I. **BECAUSE** Sec. 44(3) of the DPDP Act, 2023, travels beyond the stated object and scope of the said Act, as it traverses into the occupied field of law held by Sec. 8(1)(j) of the RTI Act, by proposing an amendment,—which suffers from the vice of overbreadth and overreach, going far beyond the statement of objects and reasons of the said Act, as well as being alien to the subject matter germane to the said Act.
  - i. The DPDP Act, 2023, is described in the Official Gazette as *“An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.”* [Emphasis supplied]

- ii. Section 2(n) defines “digital personal data” as personal data in digital form, while “personal data” is defined in Section 2(t) read with Section 3(a)(ii). Further, the definition of the term “processing” in Section 2(x) clarifies that processing of personal data refers to the use of wholly or partly automated operations performed on digital personal data for purposes specified therein. Thus, on a reading of the abovesaid four provisions, it is categorically clear that the said Act applies to digital personal data only, and not to all personal data *per se*, which may not be stored in digital form.
- iii. However, in seeking to implement the object behind the said Act, Section 44(3) has amended Section 8(1)(j) of the RTI Act in a blanket manner, sweeping within its fold all personal information, irrespective of whether such information is covered under the definition of “digital personal data” or not. As such, Section 8(1)(j) of the RTI Act, which operates not only qua “digital personal data” but is equally applicable to all kinds of information which may not even qualify as “digital personal data”, has been aggressively amended by the overzealous sweep of Section 44(3) of the DPDP Act, which is impermissible and beyond the scope of the Act.

**Section 44(3) fails the five pronged proportionality test and is an unreasonable restriction to the rights under Article 19(1)(a) and 21**

**J. BECAUSE** the unamended Section 8(1)(j) of the RTI Act, provided for the concerned PIO or Appellate Authority while dealing with personal information to conduct a public activity test, unwarranted invasion test, with a mandatory public interest override. The Petitioner submits that in permitting the concerned authorities to arrive at such a determination, the provision envisaged and inherently enabled a limited test of proportionality, which allowed for reasoned determinations as and when warranted. By amending the said provision to allow for a complete bar on the obligation to disclose personal information, the amendment creates an asymmetry which is rigid and prevents reasoned determination of larger public interest, thereby failing the constitutional safeguard of reasonableness and in turn failing the test of proportionality. The Constitution Bench judgment in *CPIO, Supreme Court of India v. Subhash Chandra Agarwal*, (2020) 5 SCC 481, had emphasized that the need for transparency in public office viz-z-viz the protected personal interest of public functionaries must be determined on a case-by-case basis, while applying the idea of open governance and using public interest as the benchmark for

balancing the competing interests. The deletion of the public interest override wherever found applicable in Section 8(1)(j) of the RTI Act makes such a balancing exercise impossible by exempting the obligation for disclosure of all personal information, which defeats the purpose behind enactment of the RTI Act. This is further exacerbated as the expansive definition of “personal data” suggests that any information which relates to personal identifiers is also exempt from disclosure. For illustration, ‘A’ may be the recipient of a subsidy/concession and under Section 4(1)(b)(xii) and 4(1)(b)(xiii) respectively of RTI Act; all information about the grant of the subsidy/concession including the entire process of decision making is liable to be disclosed. Following the amendment, not only the person’s name and other demographic and biometric details would be denied but also all information created by the public authority in the course of decision making on the application can be denied, as the information may ‘relate’ to personal data.

**K. BECAUSE** insofar as Sec 44(3) of DPDP Act eliminates the scope of reasonable determination of larger public interest in disclosure of certain personal information, it lends itself to assume the visage of an unreasonable restriction on the rights guaranteed under Article 19(1)(a) and is thus *ultra vires* the Constitution.

**Section 44(3) violates the reasonable classification test of Article 14 by treating unequals equally**

**L. BECAUSE** the amendment to Section 8(1)(j), read with the definition of “personal data” under DPDP Act, places public functionaries entrusted with public duties and ordinary citizens on an equal footing in its conceptualization of the right to privacy, which is violative of Article 14 of the Constitution. This Hon’ble Court has in numerous cases including *Association for Democratic Reforms* (2002) and *PUCL* (2003) held that the legitimate expectation of privacy of private individuals and that of people in public life entrusted with public duties cannot be equated.

**M. BECAUSE** it is no longer *res integra* that fundamental rights do not compete against each other, and co-exist harmoniously. It is therefore not open to the Parliament to prioritize one fundamental right over another by citing policy making powers. Further, the competing interests of rights and restrictions must also be harmoniously constructed and cannot allow for one interest to completely trump another in the form of blanket exemption to personal information under the amended Section 8(1)(j) of RTI Act. In *Modern Dental College & Research Centre vs State of Madhya Pradesh* (2016) 7 SCC 353, it was held in this regard,

*“...On the one hand is the right’s element, which constitutes a fundamental component of substantive democracy; on the other hand is the people element, limiting those very rights through their representatives. These two constitute a fundamental component of the notion of democracy, though this time in its formal aspect. How can this tension be resolved? The answer is that this tension is not resolved by eliminating the “losing” facet from the Constitution. Rather, the tension is resolved by way of a proper balancing of the competing principles. This is one of the expressions of the multi-faceted nature of democracy. Indeed, the inherent tension between democracy’s different facets is a “constructive tension”. It enables each facet to develop while harmoniously coexisting with the others. The best way to achieve this peaceful coexistence is through balancing between the competing interests. Such balancing enables each facet to develop alongside the other facets, not in their place. This tension between the two fundamental aspects—rights on the one hand and its limitation on the other hand—is to be resolved by balancing the two so that they harmoniously coexist with each other.” [Emphasis Supplied]*

#### **Deletion of Proviso of Section 8(1)(j) violates Article 14**

**N. BECAUSE** the deletion of the Proviso to Section 8(1)(j) of the RTI Act, 2005, is a further egress into the constitutionally protected right to know of informed voters in a representative democracy. The unamended Proviso clarified that, *“information which cannot be denied to Parliament or State Legislature cannot be denied to any person.”* The rationale behind such a proviso was a recognition that in a representative democracy there must be at the very minimum, symmetry of information between the electorate and

their representatives who are sent to Parliament / State Legislatures to act on behalf of the voters. Information which is secured by a Member of Parliament or a Member of Legislative Assembly in their capacity as elected representatives, is information received by them as trustees of the people. The representative nature of Indian polity is intrinsic to the idea of democracy and is a core element of the basic structure doctrine applicable to the Constitution of India. The DPDP Act, 2023, provides no rational basis for deletion of the Proviso to Section 8(1)(j) of the RTI Act, 2005. The subject matter of the Proviso in no way relates to processing of digital personal data, and only enshrined the principle of representative democracy operating by ensuring symmetry of information and transparency in public acts of public functionaries. The amendment through Sec. 44(3) of DPDP Act thus abrogates the right to know of electors while also creating a hierarchy between electors and their representatives about their right of access to information. Interestingly, the Union of India has argued in some litigation(s) that the Proviso is applicable to the entirety of Section 8(1) and not to Section 8(1)(j) alone, which interpretation calls into the question whether the Proviso could then have been deleted by the amendment through Section 44(3) of DPDP Act, which is limited to Section 8(1)(j) alone.

**Section 44(3) destroys the internal statutory mechanism of the RTI Act and is hit by the doctrine of arbitrariness**

- O. BECAUSE** no public consultation or legislative debate was conducted on the impact of the amendment to provisions of the RTI Act, 2005, as the amendment was not separately tabled in Parliament with specific attention on the RTI Act. Instead, through an opaque mechanism which ostensibly sought to provide digital data protection laws, the balancing features of the RTI Act built into Section 8(1)(j) were permanently altered in a manner that is ruinous to the statutory mechanism, architecture and salient purpose of the RTI Act, 2005. No rationale for such an amendment is traceable to the objects and reasons of the DPD Bill, 2023.
- P. BECAUSE** the amendment to Sec. 8(1)(j) of RTI Act, 2005, destroys the internal decision-making structure and statutory scheme of the RTI Act by extinguishing the power of the Public Information Officer and the First Appellate Authority to deploy public interest balancing criteria in cases involving personal information. This also falls foul of the judgments of this Hon'ble Court in *PUCL (2003)* and *KS Puttaswamy (2019)*
- Q. BECAUSE** retention of Section 8(2) of RTI Act, 2005, is not sufficient safeguard against the unreasonable restriction imposed

by the amended Section 8(1)(j) of RTI Act, 2005, as Section 8(2) provides for a discretionary decision regarding disclosure to be made in public interest by the public authority concerned. The section does not mandate disclosure, and more importantly, in contrast to the unamended Section 8(1)(j), instead of the CPIO / SPIO and FAA, the onus to determine whether public interest warrants disclosure has been placed on the “public authority”. While “public authority” is defined in Section 2(h) of the RTI Act, 2005, it does not include the PIO of the FAA in the definition, and it remains vague how Section 8(2) can be operationalized when RTI applications are filed. It may be pertinent to point out that there is no clarity in this regard in the Rules under the RTI Act, nor is there any Office Memorandum in this regard.

**Amendment to Section 8(1)(j) creates a conflict with statutorily mandated disclosures under Sec 4(1)(b) of RTI Act**

**R. BECAUSE** the amended Section 8(1)(j) of RTI Act, insofar as it permits blanket exemption against disclosure of personal information, is in conflict with the mandate of Section 4 of the RTI Act, which imposes obligations on public authorities to make mandatory voluntary disclosures. It is submitted that a reading of Section 4(1)(b)(viii), (ix), (x) and (xiii), makes it clear that said statutorily directed disclosures would attract the bar of personal

information, and could consequently not be published in view of the blanket exemption introduced by the amendment. This militates against the scheme of the RTI Act and is a direct blow to ideas of transparency and open governance. This Hon'ble Court in *Kishan Chand Jain vs Union of India* (2023) INSC 741 directed strict implementation of Section 4(1)(b) of RTI Act. Further in *CBSE vs Aditya Bandopadhyay* (2011) 8 SCC 497 this Hon'ble Court has held,

*“The right to information is a cherished right. Information and right to information are intended to be formidable tools in the hands of responsible citizens to fight corruption and to bring in transparency and accountability. The provisions of RTI Act should be enforced strictly and all efforts should be made to bring to light the necessary information under clause (b) of section 4(1) of the Act which relates to securing transparency and accountability in the working of public authorities and in discouraging corruption.”* [Emphasis Supplied]

**S. BECAUSE** the deletion of the balancing tests from Section 8(1)(j) of RTI Act has granted unguided and unbridled discretion to the executive to refuse disclosure of information. Such executive action has been held to be unconstitutional by this Hon'ble Court in *Anuradha Bhasin vs Union of India* (2020) 3 SCC 637.

### **Overbreadth and Vagueness**

**T. BECAUSE** the over-broad definition of the terms “data fiduciary” and “processing” in Sections 2(i) and 2(t) respectively bring within their fold investigative journalists, academics, market researchers, lawyers, social commentators, authors, educational institutions, social welfare organizations, and all other persons or entities that engage in collection, storage or dissemination of “personal data”. This is further compounded by the all-encompassing broad definition of the term “personal data” in Section 2(t) to mean, “any data in relation to an individual who is identifiable from such data.” Thus, for illustration, any collation of lists of individuals with their name, mobile number, email address, EPIC number, etc., would amount to data processing, and concomitantly would cast upon the data processor the obligations prescribed for data fiduciaries. This would cast an onerous burden of statutory compliance and red tape on individual journalists, academics, authors, lawyers, etc., rendering certain vocations so impracticable that they would be impossible to discharge. This in turn would impact and cast a chilling effect not only on the exercise of the right to freedom of speech and expression under Article 19(1)(a) but also the right to practise any trade, occupation or profession under Article 19(1)(g) of the Constitution of India. Further, the absence of any gradation between individuals and body corporates

for the purposes of imposition of penalties suggests that any data breach may lead to debilitating penalties sufficient to shut down the operation of small NGOs and think tanks which play a pivotal role in facilitating participatory democracy.

**Executive dominance in Search-cum-Selection Committees violates doctrine of separation of powers**

**U. BECAUSE** Rules 17(1) and (2) of the DPDP Rules provide for constitution of Search-cum-Selection Committees for appointment of the Chairperson and other members of the Board, wherein complete executive dominance of the Central government has been statutorily embedded. This is pertinent as the Board under the DPDP Act performs a quasi judicial function of determination of extent of data breach and the applicable penalty for the same, with penalties up to 250 Crore rupees prescribed in the Schedule. In view of the fact that the Central Government and its agents are likely to be a significant litigator before the Board, the complete dominance of the Central Government in the constitution of the Search-cum-Selection Committees violates the principle of separation of powers.

**No statutory guidance to determine what constitutes “significant” data breach**

**V. BECAUSE** Section 33(1) of DPDP Act provides that penalties may be imposed by the Board after conclusion of an inquiry when the breach of any provision of the Act and the Rules made thereunder is found to be “*significant*”. The Act and the Rules do not provide any guidance on what constitutes a “significant” breach, and what would be deemed to be a non-significant breach. Such unguided discretion in determination of application of penalty under the Act is manifestly arbitrary and violates Article 14.

**Unchecked powers to Central Government fails necessary safeguards limb of proportionality test**

**W. BECAUSE** Section 36 of the DPDP Act, gives unguided blanket power to the Central Government and requires the Board or data fiduciaries to furnish such information as may be called for by the Central Government. The Section does not even lay down any stated purpose or objective for which the information may be sought, thereby allowing for arbitrary and ad-hoc decision making by the executive without any statutory guidelines or limitations. Further, there is no appeal or review available against the order of the Central Government under Section 36 of DPDP Act. This lends the provision amenable to arbitrary and excessive abuse, with a Central Government monopoly over private data, which could in turn influence policy decisions and electoral choices, damaging the

democratic fabric of the Indian Constitution and polity. This further fails the necessary safeguards limb of the proportionality test as held in *Ramesh Chandra Sharma* (Supra).

**X. BECAUSE** the DPDP Act and the Rules made thereunder, more specifically Sec. 36 and Rule 23(1), authorizes the Central Government to call for information from data fiduciaries and intermediaries, while simultaneously under Rule 23(2) exempting the Central Government and the Data Fiduciary from informing the Data Principal, if the disclosure is deemed to affect the sovereignty and integrity of the country. In this regard, the DPDP Act and Rules do not provide for any pre-decisional hearing, nor does it provide for a review mechanism to test whether the satisfaction of the Central Government in terms of Rule 23(2) is based on cogent and valid reasons or grounds. Thus, there is no independent oversight to test the scope, duration, necessity or proportionality in the executive exercise of power, which is impermissible as held in *Anuradha Bhasin* (Supra). It is relevant to note that Rule 23 shall come into operation eighteen months after 13.11.2025, as per Rule 1(4) of the DPDP Rules.

**Y. BECAUSE** Section 17(1)(c) and 17(2)(a) empowers disproportionate surveillance by granting sweeping exemptions to both State and non-state instrumentalities to collect, preserve,

process and share data without any objective scrutiny or statutory responsibility, under the garb of crime prevention. That said, provisions virtually allow unrestricted and unqualified surveillance of all citizens without any review mechanism. Further, both the blanket exemption under 17(2)(a) and selective exemption under 17(1)(c) violate the test of proportionality for the lack of sufficient safeguards against abuse. Reliance is placed on *Gujarat Mazdoor Sabha and Anr. v State of Gujarat (2020) 10 SCC 459*.

**Z. BECAUSE** the powers under 17(1)(c) and 17(2)(a) allow indiscriminate collection and processing of data, which may be used for purposes such as predictive and algorithm based policing which have a tendency to compound prejudicial social biases. The lack of safeguards against such use of the data fails the proportionality test and renders the provisions unconstitutional.

**AA. BECAUSE** there is no reasonable nexus between the blanket exemption granted to state instrumentalities under section 17(2)(b) and the objective sought to be achieved by the DPDP Act. There is no legitimate reason to exempt state actors that conduct pervasive surveys and data processing for research and statistical purposes from being bound by the statutory obligations under the DPDP Act.

**AB.**      **BECAUSE** the Petitioner craves leave to rely on additional grounds at the stage of arguments.

### **10. PRAYER**

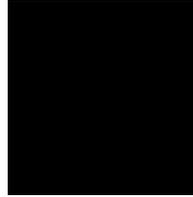
In light of the facts and circumstances stated hereinabove, and the grounds urged by the Petitioner, it is most humbly prayed that this Hon'ble Court may be pleased to:

- A.** Declare that Section 44(3) of The Digital Personal Data Protection Act, 2023, and Rule 17 of The Digital Personal Data Protection Rules, 2025 are *ultra vires* the Constitution being violative of Articles 14, 19(1)(a) and 21 of the Constitution; and
  
- B.** Declare that Sections 17(1)(c), 17(2), 33(1) and 36 of The Digital Personal Data Protection Act, 2023, as notified vide GSR 843(E) and Rule 23(2) of The Digital Personal Data Protection Rules, 2025, as notified by GSR 846(E) are *ultra vires* the Constitution being violative of Articles 14, 19(1)(a) and 21 of the Constitution; and

**C.** Pass any other order as this Hon'ble Court may deem fit and necessary.

AND FOR THIS ACT OF KINDNESS THE PETITIONER  
SHALL AS IN DUTY BOUND FOREVER PRAY

Through:



FILED

**AAKARSH KAMRA  
ADVOCATE ON RECORD**

**SETTLED BY: VRINDA GROVER, ADV**

**DRAFTED BY: SOUTIK BANERJEE, ADV  
DEVIKA TULSIANI, ADV**

**06.02.2026**

IN THE HON'BLE SUPREME COURT OF INDIA  
EXTRAORDINARY WRIT JURISTITION  
PUBLIC INTEREST LITIGATION

W.P (C) \_\_\_\_\_ / 2026

Venkatesh Nayak

.....PETITIONER

VERSUS

Union of India.

.....RESPONDENT



AFFIDAVIT

circumstances of the present case, and competent to swear this affidavit.

2. That the accompanying writ petition in public interest and the accompanying Interim Application(s) have been drafted under my instruction and the same have been shown to me after drafting, and I state that the contents of the Synopsis and List of Dates at Pages B-G Writ Petition at pages 1-33 and all accompanying Application(s) are believed to be true and correct to the best of my knowledge and belief or as per legal counsel received and information available in the public domain. The contents of Para 1-8 of the writ petition are believed to be true and correct to the best of my knowledge and belief, and the contents of Paras 9 of the writ petition are believed to be true and correct as per legal counsel, Para 10 is the humble prayer before this Hon'ble Court.

That the annexures along with the present petition are true and correct copies of their respective originals.

4. That there is no personal or vested gain, private motive or oblique reason in filing the present petition which is being filed in larger public interest.

No. of Correction Six only

5. That no similar Writ Petition seeking similar relief has been filed by the Petitioners before this Hon'ble Court or any other Court.

6. That the contents of Paras 1 to 5 hereinabove are true and correct.

### VERIFICATION

Verified at New Delhi on this 05<sup>th</sup> day of Feb 2026 that the contents of the above affidavit are true and correct to the best of my knowledge and belief, and no part of it is false and nothing material has been concealed.



SWORN TO BEFORE ME

*[Signature]*  
Y.R. CHANDRASEKAR B.Com., LL.B.  
ADVOCATE & NOTARY



05 FEB 2026

No. of Correction... nil

*[Signature]*  
Notary Stamps not affixed  
Due to non availability  
From : 01-04-2003

SL.No.....	<u>161</u>	Page.....	<u>62</u>
Vol.....	<u>I</u>	Date.....	<u>05/2/2026</u>



ANNEXURE P1

# भारत का राजपत्र The Gazette of India

सी.जी.-डी.एल.-अ.-12082023-248045  
CG-DL-E-12082023-248045

असाधारण

EXTRAORDINARY

भाग II — खण्ड 1

PART II — Section 1

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं० 25] नई दिल्ली, शुक्रवार, अगस्त 11, 2023/ श्रावण 20, 1945 (शक)  
No. 25] NEW DELHI, FRIDAY, AUGUST 11, 2023/SRAVANA 20, 1945 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।  
Separate paging is given to this Part in order that it may be filed as a separate compilation.

## MINISTRY OF LAW AND JUSTICE (Legislative Department)

*New Delhi, the 11th August, 2023/Sravana 20, 1945 (Saka)*

The following Act of Parliament received the assent of the President on the 11th August, 2023 and is hereby published for general information:—

### THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (No. 22 OF 2023)

[11th August, 2023.]

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

#### CHAPTER I

#### PRELIMINARY

1. (1) This Act may be called the Digital Personal Data Protection Act, 2023.

Short title and commencement.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Definitions.

2. In this Act, unless the context otherwise requires,—

(a) “Appellate Tribunal” means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;

24 of 1997.

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

(c) “Board” means the Data Protection Board of India established by the Central Government under section 18;

(d) “certain legitimate uses” means the uses referred to in section 7;

(e) “Chairperson” means the Chairperson of the Board;

(f) “child” means an individual who has not completed the age of eighteen years;

(g) “Consent Manager” means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform;

(h) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;

(i) “Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

(j) “Data Principal” means the individual to whom the personal data relates and where such individual is—

(i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, includes her lawful guardian, acting on her behalf;

(k) “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary;

(l) “Data Protection Officer” means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10;

(m) “digital office” means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;

(n) “digital personal data” means personal data in digital form;

(o) “gain” means—

(i) a gain in property or supply of services, whether temporary or permanent; or

(ii) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration;

(p) “loss” means—

(i) a loss in property or interruption in supply of services, whether temporary or permanent; or

(ii) a loss of opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration;

(q) “Member” means a Member of the Board and includes the Chairperson;

(r) “notification” means a notification published in the Official Gazette and the expressions “notify” and “notified” shall be construed accordingly;

(s) “person” includes—

(i) an individual;

(ii) a Hindu undivided family;

(iii) a company;

(iv) a firm;

(v) an association of persons or a body of individuals, whether incorporated or not;

(vi) the State; and

(vii) every artificial juristic person, not falling within any of the preceding sub-clauses;

(t) “personal data” means any data about an individual who is identifiable by or in relation to such data;

(u) “personal data breach” means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;

(v) “prescribed” means prescribed by rules made under this Act;

(w) “proceeding” means any action taken by the Board under the provisions of this Act;

(x) “processing” in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(y) “she” in relation to an individual includes the reference to such individual irrespective of gender;

(z) “Significant Data Fiduciary” means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10;

(za) “specified purpose” means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder; and

(zb) “State” means the State as defined under article 12 of the Constitution.

**3.** Subject to the provisions of this Act, it shall—

Application  
of Act.

(a) apply to the processing of digital personal data within the territory of India where the personal data is collected—

(i) in digital form; or

(ii) in non-digital form and digitised subsequently;

(b) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

(c) not apply to—

(i) personal data processed by an individual for any personal or domestic purpose; and

(ii) personal data that is made or caused to be made publicly available by—

(A) the Data Principal to whom such personal data relates; or

(B) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

*Illustration.*

X, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act shall not apply.

CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

Grounds for processing personal data.

4. (1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—

(a) for which the Data Principal has given her consent; or

(b) for certain legitimate uses.

(2) For the purposes of this section, the expression “lawful purpose” means any purpose which is not expressly forbidden by law.

Notice.

5. (1) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her,—

(i) the personal data and the purpose for which the same is proposed to be processed;

(ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed.

*Illustration.*

X, an individual, opens a bank account using the mobile app or website of Y, a bank. To complete the Know-Your-Customer requirements under law for opening of bank account, X opts for processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing.

(2) Where a Data Principal has given her consent for the processing of her personal data before the date of commencement of this Act,—

(a) the Data Fiduciary shall, as soon as it is reasonably practicable, give to the Data Principal a notice informing her,—

(i) the personal data and the purpose for which the same has been processed;

(ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a complaint to the Board,

in such manner and as may be prescribed.

(b) the Data Fiduciary may continue to process the personal data until and unless the Data Principal withdraws her consent.

*Illustration.*

X, an individual, gave her consent to the processing of her personal data for an online shopping app or website operated by Y, an e-commerce service provider, before the commencement of this Act. Upon commencement of the Act, Y shall, as soon as practicable, give through email, in-app notification or other effective method information to X, describing the personal data and the purpose of its processing.

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

6. (1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Consent.

*Illustration.*

X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for (i) the processing of her personal data for making available telemedicine services, and (ii) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services.

(2) Any part of consent referred in sub-section (1) which constitutes an infringement of the provisions of this Act or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement.

*Illustration.*

X, an individual, buys an insurance policy using the mobile app or website of Y, an insurer. She gives to Y her consent for (i) the processing of her personal data by Y for the purpose of issuing the policy, and (ii) waiving her right to file a complaint to the Data Protection Board of India. Part (ii) of the consent, relating to waiver of her right to file a complaint, shall be invalid.

(3) Every request for consent under the provisions of this Act or the rules made thereunder shall be presented to the Data Principal in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act.

(4) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.

(5) The consequences of the withdrawal referred to in sub-section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

*Illustration.*

X, an individual, is the user of an online shopping app or website operated by Y, an e-commerce service provider. X consents to the processing of her personal data by Y for the purpose of fulfilling her supply order and places an order for supply of a good while making payment for the same. If X withdraws her consent, Y may stop enabling X to use the app or website for placing orders, but may not stop the processing for supply of the goods already ordered and paid for by X.

(6) If a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.

*Illustration.*

X, a telecom service provider, enters into a contract with Y, a Data Processor, for emailing telephone bills to the customers of X. Z, a customer of X, who had earlier given her consent to X for the processing of her personal data for emailing of bills, downloads the mobile app of X and opts to receive bills only on the app. X shall itself cease, and shall cause Y to cease, the processing of the personal data of Z for emailing bills.

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

(8) The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.

(9) Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.

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

Certain  
legitimate uses.

7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:—

(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.

*Illustrations.*

(I) X, an individual, makes a purchase at Y, a pharmacy. She voluntarily provides Y her personal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt.

(II) X, an individual, electronically messages Y, a real estate broker, requesting Y to help identify a suitable rented accommodation for her and shares her personal data for this purpose. Y may process her personal data to identify and intimate to her the details of accommodation available on rent. Subsequently, X informs Y that X no longer needs help from Y. Y shall cease to process the personal data of X;

(b) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where—

(i) she has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(ii) such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government,

subject to standards followed for processing being in accordance with the policy issued by the Central Government or any law for the time being in force for governance of personal data.

*Illustration.*

X, a pregnant woman, enrolls herself on an app or website to avail of government's maternity benefits programme, while consenting to provide her personal data for the purpose of availing of such benefits. Government may process the personal data of X processing to determine her eligibility to receive any other prescribed benefit from the government;

(c) for the performance by the State or any of its instrumentalities of 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;

(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(e) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

(f) 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;

(g) 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;

(h) for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

*Explanation.*—For the purposes of this clause, the expression “disaster” shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005; or

53 of 2005.

(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

8. (1) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.

General obligations of Data Fiduciary.

(2) A Data Fiduciary may 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 only under a valid contract.

(3) Where personal data processed by a Data Fiduciary is likely to be—

(a) used to make a decision that affects the Data Principal; or

(b) disclosed to another Data Fiduciary,

the Data Fiduciary processing such personal data shall ensure its completeness, accuracy and consistency.

(4) A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.

(5) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

(6) In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.

(7) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—

(a) erase personal data, upon the Data Principal withdrawing her consent or as

soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and

(b) cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for processing to such Data Processor.

*Illustrations.*

(I) X, an individual, registers herself on an online marketplace operated by Y, an e-commerce service provider. X gives her consent to Y for the processing of her personal data for selling her used car. The online marketplace helps conclude the sale. Y shall no longer retain her personal data.

(II) X, an individual, decides to close her savings account with Y, a bank. Y is required by law applicable to banks to maintain the record of the identity of its clients for a period of ten years beyond closing of accounts. Since retention is necessary for compliance with law, Y shall retain X's personal data for the said period.

(8) The purpose referred to in clause (a) of sub-section (7) shall be deemed to no longer be served, if the Data Principal does not—

(a) approach the Data Fiduciary for the performance of the specified purpose; and

(b) exercise any of her rights in relation to such processing,

for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.

(9) A Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of her personal data.

(10) A Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals.

(11) For the purposes of this section, it is hereby clarified that a Data Principal shall be considered as not having approached the Data Fiduciary for the performance of the specified purpose, in any period during which she has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical form.

Processing of personal data of children.

**9.** (1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed.

*Explanation.*—For the purpose of this sub-section, the expression “consent of the parent” includes the consent of lawful guardian, wherever applicable.

(2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.

(3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

(4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.

(5) The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify.

Additional obligations of Significant Data Fiduciary.

**10.** (1) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including—

- (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.

(2) The Significant Data Fiduciary shall—

(a) appoint a Data Protection Officer who shall—

(i) represent the Significant Data Fiduciary under the provisions of this Act;

(ii) be based in India;

(iii) be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary; and

(iv) be the point of contact for the grievance redressal mechanism under the provisions of this Act;

(b) appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act; and

(c) undertake the following other measures, namely:—

(i) periodic Data Protection Impact Assessment, which shall be a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed;

(ii) periodic audit; and

(iii) such other measures, consistent with the provisions of this Act, as may be prescribed.

### CHAPTER III

#### RIGHTS AND DUTIES OF DATA PRINCIPAL

**11.** (1) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (a) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed,—

Right to access information about personal data.

(a) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;

(b) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(c) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

(2) Nothing contained in clause (b) or clause (c) of sub-section (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where 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.

Right to correction and erasure of personal data.

**12.** (1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal,—

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

(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

Right of grievance redressal.

**13.** (1) A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act and the rules made thereunder.

(2) The Data Fiduciary or Consent Manager shall respond to any grievances referred to in sub-section (1) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.

(3) The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board.

Right to nominate.

**14.** (1) A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act and the rules made thereunder.

(2) For the purposes of this section, the expression “incapacity” means inability to exercise the rights of the Data Principal under the provisions of this Act or the rules made thereunder due to unsoundness of mind or infirmity of body.

Duties of Data Principal.

**15.** A Data Principal shall perform the following duties, namely:—

- (a) comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act;
- (b) to ensure not to impersonate another person while providing her personal data for a specified purpose;
- (c) to ensure not to suppress any material information while providing her personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;
- (d) to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and
- (e) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made thereunder.

## CHAPTER IV

## SPECIAL PROVISIONS

**16.** (1) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

Processing of personal data outside India.

(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

**17.** (1) The provisions of Chapter II, except sub-sections (1) and (5) of section 8, and those of Chapter III and section 16 shall not apply where—

Exemptions.

(a) the processing of personal data is necessary for enforcing any legal right or claim;

(b) the processing of personal data by any court or tribunal or any other body in India 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;

(c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India;

(d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India;

(e) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force; and

(f) the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.

*Explanation.*—For the purposes of this clause, the expressions “default” and “financial institution” shall have the meanings respectively assigned to them in sub-sections (12) and (14) of section 3 of the Insolvency and Bankruptcy Code, 2016.

31 of 2016.

*Illustration.*

X, an individual, takes a loan from Y, a bank. X defaults in paying her monthly loan repayment instalment on the date on which it falls due. Y may process the personal data of X for ascertaining her financial information and assets and liabilities.

(2) The provisions of this Act shall not apply in respect of the processing of personal data—

(a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and

(b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.

(3) The Central Government may, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries, including startups, as Data Fiduciaries to whom the provisions of section 5, sub-sections (3) and (7) of section 8 and sections 10 and 11 shall not apply.

*Explanation.*—For the purposes of this sub-section, the term “startup” means a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.

(4) In respect of processing by the State or any instrumentality of the State, the provisions of sub-section (7) of section 8 and sub-section (3) of section 12 and, where such processing is for a purpose that does not include making of a decision that affects the Data Principal, sub-section (2) of section 12 shall not apply.

(5) The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification.

## CHAPTER V

### DATA PROTECTION BOARD OF INDIA

Establishment  
of Board.

**18.** (1) With effect from such date as the Central Government may, by notification, appoint, there shall be established, for the purposes of this Act, a Board to be called the Data Protection Board of India.

(2) The Board shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

(3) The headquarters of the Board shall be at such place as the Central Government may notify.

Composition  
and  
qualifications  
for  
appointment  
of  
Chairperson  
and Members.

**19.** (1) The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify.

(2) The Chairperson and other Members shall be appointed by the Central Government in such manner as may be prescribed.

(3) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

Salary,  
allowances  
payable to and  
term of  
office.

**20.** (1) The salary, allowances and other terms and conditions of service of the Chairperson and other Members shall be such as may be prescribed, and shall not be varied to their disadvantage after their appointment.

(2) The Chairperson and other Members shall hold office for a term of two years and shall be eligible for re-appointment.

- 21.** (1) A person shall be disqualified for being appointed and continued as the Chairperson or a Member, if she—
- (a) has been adjudged as an insolvent;
- (b) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;
- (c) has become physically or mentally incapable of acting as a Member;
- (d) has acquired such financial or other interest, as is likely to affect prejudicially her functions as a Member; or
- (e) has so abused her position as to render her continuance in office prejudicial to the public interest.
- (2) The Chairperson or Member shall not be removed from her office by the Central Government unless she has been given an opportunity of being heard in the matter.
- 22.** (1) The Chairperson or any other Member may give notice in writing to the Central Government of resigning from her office, and such resignation shall be effective from the date on which the Central Government permits her to relinquish office, or upon expiry of a period of three months from the date of receipt of such notice, or upon a duly appointed successor entering upon her office, or upon the expiry of the term of her office, whichever is earliest.
- (2) A vacancy caused by the resignation or removal or death of the Chairperson or any other Member, or otherwise, shall be filled by fresh appointment in accordance with the provisions of this Act.
- (3) The Chairperson and any other Member shall not, for a period of one year from the date on which they cease to hold such office, except with the previous approval of the Central Government, accept any employment, and shall also disclose to the Central Government any subsequent acceptance of employment with any Data Fiduciary against whom proceedings were initiated by or before such Chairperson or other Member.
- 23.** (1) The Board shall observe such procedure in regard to the holding of and transaction of business at its meetings, including by digital means, and authenticate its orders, directions and instruments in such manner as may be prescribed.
- (2) No act or proceeding of the Board shall be invalid merely by reason of—
- (a) any vacancy in or any defect in the constitution of the Board;
- (b) any defect in the appointment of a person acting as the Chairperson or other Member of the Board; or
- (c) any irregularity in the procedure of the Board, which does not affect the merits of the case.
- (3) When the Chairperson is unable to discharge her functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson until the date on which the Chairperson resumes her duties.
- 24.** The Board may, with previous approval of the Central Government, appoint such officers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of this Act, on such terms and conditions of appointment and service as may be prescribed.
- 25.** The Chairperson, Members, officers and employees of the Board shall be deemed, when acting or purporting to act in pursuance of provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.

Disqualifications for appointment and continuation as Chairperson and Members of Board.

Resignation by Members and filling of vacancy.

Proceedings of Board.

Officers and employees of Board.

Members and officers to be public servants.

Powers of  
Chairperson.

**26.** The Chairperson shall exercise the following powers, namely:—

(a) general superintendence and giving direction in respect of all administrative matters of the Board;

(b) authorise any officer of the Board to scrutinise any intimation, complaint, reference or correspondence addressed to the Board; and

(c) authorise performance of any of the functions of the Board and conduct any of its proceedings, by an individual Member or groups of Members and to allocate proceedings among them.

## CHAPTER VI

### POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD

Powers and  
functions of  
Board.

**27.** (1) The Board shall exercise and perform the following powers and functions, namely:—

(a) on receipt of an intimation of personal data breach under sub-section (6) of section 8, to direct any urgent remedial or mitigation measures in the event of a personal data breach, and to inquire into such personal data breach and impose penalty as provided in this Act;

(b) on a complaint made by a Data Principal in respect of a personal data breach or a breach in observance by a Data Fiduciary of its obligations in relation to her personal data or the exercise of her rights under the provisions of this Act, or on a reference made to it by the Central Government or a State Government, or in compliance of the directions of any court, to inquire into such breach and impose penalty as provided in this Act;

(c) on a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to her personal data, to inquire into such breach and impose penalty as provided in this Act;

(d) on receipt of an intimation of breach of any condition of registration of a Consent Manager, to inquire into such breach and impose penalty as provided in this Act; and

(e) on a reference made by the Central Government in respect of the breach in observance of the provisions of sub-section (2) of section 37 by an intermediary, to inquire into such breach and impose penalty as provided in this Act.

(2) The Board may, for the effective discharge of its functions under the provisions of this Act, after giving the person concerned an opportunity of being heard and after recording reasons in writing, issue such directions as it may consider necessary to such person, who shall be bound to comply with the same.

(3) The Board may, on a representation made to it by a person affected by a direction issued under sub-section (1) or sub-section (2), or on a reference made by the Central Government, modify, suspend, withdraw or cancel such direction and, while doing so, impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

Procedure to  
be followed by  
Board.

**28.** (1) The Board shall function as an independent body and shall, as far as practicable, function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures as may be prescribed.

(2) The Board may, on receipt of an intimation or complaint or reference or directions as referred to in sub-section (1) of section 27, take action in accordance with the provisions of this Act and the rules made thereunder.

(3) The Board shall determine whether there are sufficient grounds to proceed with an inquiry.

(4) In case the Board determines that there are insufficient grounds, it may, for reasons to be recorded in writing, close the proceedings.

(5) In case the Board determines that there are sufficient grounds to proceed with inquiry, it may, for reasons to be recorded in writing, inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the provisions of this Act.

(6) The Board shall conduct such inquiry following the principles of natural justice and shall record reasons for its actions during the course of such inquiry.

5 of 1908.

(7) For the purposes of discharging its functions under this Act, the Board shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to—

(a) summoning and enforcing the attendance of any person and examining her on oath;

(b) receiving evidence of affidavit requiring the discovery and production of documents;

(c) inspecting any data, book, document, register, books of account or any other document; and

(d) such other matters as may be prescribed.

(8) The Board or its officers shall not prevent access to any premises or take into custody any equipment or any item that may adversely affect the day-to-day functioning of a person.

(9) The Board may require the services of any police officer or any officer of the Central Government or a State Government to assist it for the purposes of this section and it shall be the duty of every such officer to comply with such requisition.

(10) During the course of the inquiry, if the Board considers it necessary, it may for reasons to be recorded in writing, issue interim orders after giving the person concerned an opportunity of being heard.

(11) On completion of the inquiry and after giving the person concerned an opportunity of being heard, the Board may for reasons to be recorded in writing, either close the proceedings or proceed in accordance with section 33.

(12) At any stage after receipt of a complaint, if the Board is of the opinion that the complaint is false or frivolous, it may issue a warning or impose costs on the complainant.

## CHAPTER VII

### APPEAL AND ALTERNATE DISPUTE RESOLUTION

**29.** (1) Any person aggrieved by an order or direction made by the Board under this Act may prefer an appeal before the Appellate Tribunal.

Appeal to  
Appellate  
Tribunal.

(2) Every appeal under sub-section (1) shall be filed within a period of sixty days from the date of receipt of the order or direction appealed against and it shall be in such form and manner and shall be accompanied by such fee as may be prescribed.

(3) The Appellate Tribunal may entertain an appeal after the expiry of the period specified in sub-section (2), if it is satisfied that there was sufficient cause for not preferring the appeal within that period.

(4) On receipt of an appeal under sub-section (1), the Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the Board and to the parties to the appeal.

(6) The appeal filed before the Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date on which the appeal is presented to it.

(7) Where any appeal under sub-section (6) could not be disposed of within the period of six months, the Appellate Tribunal shall record its reasons in writing for not disposing of the appeal within that period.

(8) Without prejudice to the provisions of section 14A and section 16 of the Telecom Regulatory Authority of India Act, 1997, the Appellate Tribunal shall deal with an appeal under this section in accordance with such procedure as may be prescribed. 24 of 1997.

(9) Where an appeal is filed against the orders of the Appellate Tribunal under this Act, the provisions of section 18 of the Telecom Regulatory Authority of India Act, 1997 shall apply. 24 of 1997.

(10) In respect of appeals filed under the provisions of this Act, the Appellate Tribunal shall, as far as practicable, function as a digital office, with the receipt of appeal, hearing and pronouncement of decisions in respect of the same being digital by design.

Orders passed by Appellate Tribunal to be executable as decree.

**30.** (1) An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

Alternate dispute resolution.

**31.** If the Board is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any law for the time being in force in India.

Voluntary undertaking.

**32.** (1) The Board may accept a voluntary undertaking in respect of any matter related to observance of the provisions of this Act from any person at any stage of a proceeding under section 28.

(2) The voluntary undertaking referred to in sub-section (1) may include an undertaking to take such action within such time as may be determined by the Board, or refrain from taking such action, and or publicising such undertaking.

(3) The Board may, after accepting the voluntary undertaking and with the consent of the person who gave the voluntary undertaking vary the terms included in the voluntary undertaking.

(4) The acceptance of the voluntary undertaking by the Board shall constitute a bar on proceedings under the provisions of this Act as regards the contents of the voluntary undertaking, except in cases covered by sub-section (5).

(5) Where a person fails to adhere to any term of the voluntary undertaking accepted by the Board, such breach shall be deemed to be breach of the provisions of this Act and the Board may, after giving such person an opportunity of being heard, proceed in accordance with the provisions of section 33.

## CHAPTER VIII

### PENALTIES AND ADJUDICATION

Penalties.

**33.** (1) If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the

person an opportunity of being heard, impose such monetary penalty specified in the Schedule.

(2) While determining the amount of monetary penalty to be imposed under sub-section (1), the Board shall have regard to the following matters, namely:—

(a) the nature, gravity and duration of the breach;

(b) the type and nature of the personal data affected by the breach;

(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) whether the person took any action to mitigate the effects and consequences of the breach, and 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 provisions of this Act; and

(g) the likely impact of the imposition of the monetary penalty on the person.

**34.** All sums realised by way of penalties imposed by the Board under this Act, shall be credited to the Consolidated Fund of India.

Crediting sums realised by way of penalties to Consolidated Fund of India.

## CHAPTER IX

### MISCELLANEOUS

**35.** No suit, prosecution or other legal proceedings shall lie against the Central Government, the Board, its Chairperson and any Member, officer or employee thereof for anything which is done or intended to be done in good faith under the provisions of this Act or the rules made thereunder.

Protection of action taken in good faith.

**36.** The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

Power to call for information.

**37.** (1) The Central Government or any of its officers specially authorised by it in this behalf may, upon receipt of a reference in writing from the Board that—

Power of Central Government to issue directions.

(a) intimates the imposition of monetary penalty by the Board on a Data Fiduciary in two or more instances; and

(b) advises, in the interests of the general public, the blocking for access by the public to any information generated, transmitted, received, stored or hosted, in any computer resource that enables such Data Fiduciary to carry on any activity relating to offering of goods or services to Data Principals within the territory of India,

after giving an opportunity of being heard to that Data Fiduciary, on being satisfied that it is necessary or expedient so to do, in the interests of the general public, for reasons to be recorded in writing, by order, direct any agency of the Central Government or any intermediary to block for access by the public or cause to be blocked for access by the public any such information.

(2) Every intermediary who receives a direction issued under sub-section (1) shall be bound to comply with the same.

(3) For the purposes of this section, the expressions “computer resource”, “information” and “intermediary” shall have the meanings respectively assigned to them in the Information Technology Act, 2000.

Consistency with other laws.

**38.** (1) The provisions of this Act shall be in addition to and not in derogation of any other law for the time being in force.

(2) In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

Bar of jurisdiction.

**39.** No civil court shall have the jurisdiction to entertain any suit or proceeding in respect of any matter for which the Board is empowered under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power under the provisions of this Act.

Power to make rules.

**40.** (1) The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act.

(2) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(a) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (1) of section 5;

(b) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (2) of section 5;

(c) the manner of accountability and the obligations of Consent Manager under sub-section (8) of section 6;

(d) the manner of registration of Consent Manager and the conditions relating thereto, under sub-section (9) of section 6;

(e) the subsidy, benefit, service, certificate, licence or permit for the provision or issuance of which, personal data may be processed under clause (b) of section 7;

(f) the form and manner of intimation of personal data breach to the Board under sub-section (6) of section 8;

(g) the time period for the specified purpose to be deemed as no longer being served, under sub-section (8) of section 8;

(h) the manner of publishing the business contact information of a Data Protection Officer under sub-section (9) of section 8;

(i) the manner of obtaining verifiable consent under sub-section (1) of section 9;

(j) the classes of Data Fiduciaries, the purposes of processing of personal data of a child and the conditions relating thereto, under sub-section (4) of section 9;

(k) the other matters comprising the process of Data Protection Impact Assessment under sub-clause (i) of clause (c) of sub-section (2) of section 10;

(l) the other measures that the Significant Data Fiduciary shall undertake under sub-clause (iii) of clause (c) of sub-section (2) of section 10;

(m) the manner in which a Data Principal shall make a request to the Data Fiduciary to obtain information and any other information related to the personal data of such Data Principal and its processing, under sub-section (1) of section 11;

(n) the manner in which a Data Principal shall make a request to the Data Fiduciary for erasure of her personal data under sub-section (3) of section 12;

(o) the period within which the Data Fiduciary shall respond to any grievances under sub-section (2) of section 13;

(p) the manner of nomination of any other individual by the Data Principal under sub-section (1) of section 14;

(q) the standards for processing the personal data for exemption under clause (b) of sub-section (2) of section 17;

(r) the manner of appointment of the Chairperson and other Members of the Board under sub-section (2) of section 19;

(s) the salary, allowances and other terms and conditions of services of the Chairperson and other Members of the Board under sub-section (1) of section 20;

(t) the manner of authentication of orders, directions and instruments under sub-section (1) of section 23;

(u) the terms and conditions of appointment and service of officers and employees of the Board under section 24;

(v) the techno-legal measures to be adopted by the Board under sub-section (1) of section 28;

(w) the other matters under clause (d) of sub-section (7) of section 28;

(x) the form, manner and fee for filing an appeal under sub-section (2) of section 29;

(y) the procedure for dealing an appeal under sub-section (8) of section 29;

(z) any other matter which is to be or may be prescribed or in respect of which provision is to be, or may be, made by rules.

**41.** Every rule made and every notification issued under section 16 and section 42 of this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or notification or both Houses agree that the rule or notification should not be made or issued, the rule or notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or notification.

Laying of rules and certain notifications.

**42.** (1) The Central Government may, by notification, amend the Schedule, subject to the restriction that no such notification shall have the effect of increasing any penalty specified therein to more than twice of what was specified in it when this Act was originally enacted.

Power to amend Schedule.

(2) Any amendment notified under sub-section (1) shall have effect as if enacted in this Act and shall come into force on the date of the notification.

**43.** (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the difficulty.

Power to remove difficulties.

(2) No order as referred to in sub-section (1) shall be made after the expiry of three years from the date of commencement of this Act.

(3) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

24 of 1997.

**44.** (1) In section 14 of the Telecom Regulatory Authority of India Act, 1997, in clause (c), for sub-clauses (i) and (ii), the following sub-clauses shall be substituted, namely:—

Amendments to certain Acts.

- “(i) the Appellate Tribunal under the Information Technology Act, 2000; 21 of 2000.
- (ii) the Appellate Tribunal under the Airports Economic Regulatory Authority of India Act, 2008; and 27 of 2008.
- (iii) the Appellate Tribunal under the Digital Personal Data Protection Act, 2023.”.
- (2) The Information Technology Act, 2000 shall be amended in the following manner, namely:— 21 of 2000.
- (a) section 43A shall be omitted;
- (b) in section 81, in the proviso, after the words and figures “the Patents Act, 1970”, the words and figures “or the Digital Personal Data Protection Act, 2023” shall be inserted; and 39 of 1970.
- (c) in section 87, in sub-section (2), clause (ob) shall be omitted.
- (3) In section 8 of the Right to Information Act, 2005, in sub-section (1), for clause (j), the following clause shall be substituted, namely:— 22 of 2005.
- “(j) information which relates to personal information;”.

## 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.

DR. REETA VASISHTA,  
Secretary to the Govt. of India.

ANNEXURE P2



# भारत का राजपत्र

## The Gazette of India

सी.जी.-डी.एल.-अ.-14112025-267647  
CG-DL-E-14112025-267647

असाधारण  
EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)  
PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित  
PUBLISHED BY AUTHORITY

सं. 757]

नई दिल्ली, बृहस्पतिवार, नवम्बर 13, 2025/ कार्तिक 22, 1947

No. 757]

NEW DELHI, THURSDAY, NOVEMBER 13, 2025/ KARTIKA 22, 1947

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय

अधिसूचना

नई दिल्ली, 13 नवम्बर, 2025

सा.का.नि. 843(अ).—डिजिटल वैयक्तिक डेटा संरक्षण अधिनियम, 2023 (2023 का 22 वां) की धारा 1 की उपधारा (2) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, केंद्र सरकार एतद्वारा निर्धारित करती है कि-

(क) इस अधिसूचना के भारत के राजपत्र में प्रकाशन की तिथि से, उक्त अधिनियम की धारा 1 की उप-धारा (2), धारा 2, धाराएँ 18 से 26, धाराएँ 35, 38, 39, 40, 41, 42, 43 तथा धारा 44 की उप-धाराएँ (1) और (3) प्रवृत्त होंगी;

(ख) इस राजपत्र के प्रकाशन की तिथि से एक वर्ष, जिस दिन उक्त अधिनियम की धारा 6 की उपधारा (9) और धारा 27 की उपधारा (1) के खंड (घ) के प्रावधान लागू होंगे।

(ग) इस राजपत्र के प्रकाशन की तिथि से अठारह महीने, जिस पर धारा 3 से 5, धारा 6 की उपधारा (1) से (8) और (10), धारा 7 से 10, धारा 11 से 17, धारा 27 (उपर्युक्त धारा की उपधारा (1) के खंड (घ) को छोड़कर), धारा 28 से 34, 36, 37 और उक्त अधिनियम की धारा 44 की उपधारा (2) के प्रावधान लागू होंगे।

[फा.सं. AA-11038/1/2025- सी एल और ई एस]

अजीत कुमार, संयुक्त सचिव

**MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY**  
**NOTIFICATION**

New Delhi, the 13th November, 2025

**G.S.R. 843(E).**—In exercise of the powers conferred by sub-section (2) of section 1 of the Digital Personal Data Protection Act, 2023 (22 of 2023), the Central Government hereby appoints—

- (a) the date of publication of this notification in the Official Gazette as the date on which the provisions of sub-section (2) of section 1, section 2, sections 18 to 26 sections 35, 38, 39, 40, 41, 42, 43, and sub-sections (1) and (3) of section 44 of the said Act shall come into force;
- (b) one year from the date of publication of this gazette on which the provisions of sub-section (9) of section 6 and clause (d) of sub-section (1) of section 27 of the said Act shall come into force.
- (c) eighteen months from the date of publication of this gazette, on which the provision of sections 3 to 5, sub-sections (1) to (8) and (10) of section 6, sections 7 to 10, sections 11 to 17, section 27 except clause (d) of sub-section (1) of the said section, sections 28 to 34, 36, 37 and sub-section (2) of section 44 of the said Act shall come into force.

[F. No. AA-11038/1/2025-CL&ES]

AJIT KUMAR, Jt. Secy.

**MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY**

**NOTIFICATION**

New Delhi, the 13th November, 2025

**ANNEXURE P3**

**G.S.R. 846(E).**— Whereas draft of the Digital Personal Data Protection Rules, 2025 were published, as required under sub-section (1) of section 40 of the of the Digital Personal Data Protection Act, 2023 (22 of 2023), *vide* notification of the Government of India in the Ministry of Electronics and Information Technology *vide* number G.S.R. 02 (E), dated the 3<sup>rd</sup> January, 2025, in the Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i), dated the 3<sup>rd</sup> January, 2025, inviting objections and suggestions from all persons likely to be affected thereby, before the expiry of the period of forty-five days from the date on which copies of the Official Gazette containing the said notification were made available to public;

And whereas copies of the said Official Gazette were made available to the public on the 3<sup>rd</sup> January, 2025;

And whereas objections and suggestions were received from the public in respect of the said draft rules have been considered by the Central Government;

Now, therefore in exercise of powers conferred by sub-sections (1) and (2) of section 40 of the Digital Personal Data Protection Act, 2023 (22 of 2023), the Central Government hereby makes the following rules, namely: —

**1. Short title and commencement.** — (1) These rules may be called the Digital Personal Data Protection Rules, 2025.

(2) Rules 1, 2 and 17 to 21 shall come into force on the date of their publication in the Official Gazette.

(3) Rule 4 shall come into force one year after the date of publication of this Gazette.

(4) Rules 3, 5 to 16, 22 and 23 shall come into force eighteen months after the date of publication of this Gazette.

**2. Definitions.** — (1) In these rules, unless the context otherwise requires, —

(a) “Act” means the Digital Personal Data Protection Act, 2023 (22 of 2023);

(b) “techno-legal measures” means as referred to under rules 20 and 22;

(c) “user account” means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary; and

(d) “verifiable consent” means a consent as specified in rule 10 or 11.

(2) The words and expressions used in these rules and not defined, but defined in the Act, shall have the same meanings respectively assigned to them in the Act.

**3. Notice given by Data Fiduciary to Data Principal.** —The notice given by the Data Fiduciary to the Data Principal shall—

(a) be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary;

(b) give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum, —

(i) an itemised description of such personal data; and

(ii) the specified purpose or purposes of, and specific description of the goods or services to be provided or uses to be enabled by, such processing; and

(c) give, the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may—

- (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given;
- (ii) exercise her rights under the Act; and
- (iii) make a complaint to the Board.

**4. Registration and obligations of Consent Manager.** — (1) A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website.

(2) On receipt of such application, the Board may make such inquiry as it may deem fit to satisfy itself regarding fulfilment of the conditions set out in Part A of First Schedule, and if it—

- (a) is satisfied, register the applicant as a Consent Manager, under intimation to the applicant, and publish on its website the particulars of such Consent Manager; or
- (b) is not satisfied, reject the application and communicate the reasons for the rejection to the applicant.

(3) The Consent Manager shall have obligations as specified in Part B of First Schedule.

(4) If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under this rule, 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.

(5) The Board may, if it is satisfied that it is necessary so to do in the interests of Data Principals, after giving the Consent Manager an opportunity of being heard, by order, for reasons to be recorded 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, to protect the interests of the Data Principals.

(6) The Board may, for the purposes of this rule, require the Consent Manager to furnish such information as the Board may call for.

**5. Processing of personal data for provision or issue of subsidy, benefit, service, certificate, licence or permit by State and its instrumentalities.** — (1) Processing the personal data of a Data Principal under this rule shall be done following the standards specified in Second Schedule.

(2) In this rule and the Second Schedule, the reference to any subsidy, benefit, service, certificate, licence or permit that is provided or issued—

- (a) under law shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit in exercise of any power of or the performance of any function by the State or any of its instrumentalities under any law for the time being in force;
- (b) under policy shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit 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 shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit by incurring expenditure on the same from, or with accrual of receipts to, —

- (i) in case of the Central Government or a State Government, the Consolidated Fund of India or the Consolidated Fund of the State or the public account of India or the public account of the State; or
- (ii) 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.

**6. Reasonable security safeguards.** — (1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum, —

- (a) 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) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor, wherever applicable;
- (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) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, such as by way of data-backups;
- (e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;
- (f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor, wherever applicable, for taking reasonable security safeguards; and
- (g) appropriate technical and organisational measures to ensure effective observance of security safeguards.

(2) In this rule, the expression “computer resource” shall have the same meaning as is assigned to it in Information Technology Act, 2000 (21 of 2000).

**7. Intimation of personal data breach.** — (1) On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary, —

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

(2) On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board, —

- (a) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact;
- (b) within seventy-two hours of becoming aware of the breach, or within such longer period as the Board may allow on a request made in writing in this behalf, —
  - (i) updated and detailed information in respect of such description;
  - (ii) the broad facts related to the events, circumstances and reasons leading to the breach;
  - (iii) measures implemented or proposed, if any, to mitigate risk;
  - (iv) any findings regarding the person who caused the breach;
  - (v) remedial measures taken to prevent recurrence of such breach; and
  - (vi) a report regarding the intimations given to affected Data Principals.

**8. Time period for specified purpose to be deemed as no longer being served.**—(1) A Data Fiduciary, who is of such class and is processing personal data for such corresponding purposes as are specified in Third Schedule, shall erase such personal data, unless its retention is necessary for compliance with any law for the time being in force, or, for the corresponding time period specified in the Third Schedule, if the Data Principal neither approaches such Data Fiduciary for the performance of the specified purpose nor exercises her rights in relation to such processing.

(2) At least forty-eight hours before completion of the time period for erasure of personal data under this rule, the Data Fiduciary shall inform the Data Principal that such personal data shall be erased upon completion of such period, unless she logs into her user account or otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises her rights in relation to the processing of such personal data.

(3) Without prejudice to sub-rules (1) and (2), a Data Fiduciary shall retain, in respect of any processing of personal data undertaken by it or on its behalf by a Data Processor, such 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 as specified in the Seventh Schedule, after which the Data Fiduciary shall cause such personal data and logs to be erased, unless further retention is required for compliance with any other law for the time being in force or notified by the Government.

*Illustration.*

Case 1: X, a Data Principal purchases an e-book on an e-book platform Y. Once delivery is completed, the specified purpose of processing is served. The platform Y must retain the order details, personal data, and logs of the processing (such as order confirmation, payment, and delivery events) for at least one year from the date of the transaction, even if X deletes her account.

Case 2: X, a company engages a cloud service provider C as its Data Processor to host customer records. X as the Data Fiduciary, is required to ensure that the C also retains the data and associated logs for at least one year before erasure, unless any other applicable law requires a longer period.

**9. Contact information of person to answer questions about processing.**— Every Data Fiduciary shall prominently publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data.

**10. Verifiable consent for processing of personal data of child.**—(1) A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to—

(a) reliable details of identity and age of the individual available with the Data Fiduciary; or

(b) details of identity and age, voluntarily provided —

(i) by the individual; or

(ii) through a virtual token mapped to such details, which is issued by an authorised entity.

(2) In this rule, the expression—

(a) “adult” shall mean an individual who has completed the age of eighteen years;

(b) “authorised entity” shall mean —

(i) an entity entrusted by law or 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; or

- (ii) a person appointed or permitted by the entity specified under clause (i), for such issuance, and also includes details of identity and age or token made available and verified by a Digital Locker Service Provider;
- (c) “Digital Locker service provider” shall mean such intermediary, including a body corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000);

*Illustration.*

C is a child, P is a parent, and DF is a Data Fiduciary. A user account of C is sought to be created on the online platform of DF, by processing the personal data of C.

*Case 1:* C informs DF that she is a child and declares P as her parent. DF shall enable P to identify herself through its website, app or other appropriate means. P identifies herself as the parent and informs DF that she is a registered user on DF’s platform and has previously made available her identity and age details to DF. Before processing C’s personal data for the creation of her user account, DF shall check to confirm that it holds reliable identity and age details of P and that P is an identifiable adult.

*Case 2:* C informs DF that she is a child and declares P as her parent. DF shall enable P to identify herself through its website, app or other appropriate means. P identifies herself as the parent and informs DF that she herself is not a registered user on DF’s platform. Before processing C’s personal data for the creation of her user account, DF shall, by reference to identity and age details issued by an entity entrusted by law or the Government with maintenance of the said details or to a virtual token mapped to the identity and age, check that P is an identifiable adult. P may voluntarily make such details available using the services of a Digital Locker service provider.

*Case 3:* P is opening an account for C and identifies herself as C’s parent and informs DF that she is a registered user on DF’s platform and has previously made available her identity and age details to DF. Before processing C’s personal data for the creation of her user account, DF shall check to confirm that it holds reliable identity and age details of P and that P is an identifiable adult.

*Case 4:* P is opening an account for C and identifies herself as C’s parent and informs DF that she herself is not a registered user on DF’s platform. Before processing C’s personal data for the creation of her user account, DF shall, by reference to identity and age details issued by an entity entrusted by law or the Government with maintenance of the said details or to a virtual token mapped to the identity and age, check that P is an identifiable adult. P may voluntarily make such details available using the services of a Digital Locker service provider.

**11. Verifiable consent for processing of personal data of person with disability who has lawful guardian.** — (1) A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, or by a designated authority or by a local level committee, under the law applicable to guardianship.

(2) In this rule, the expression—

- (a) “designated authority” shall mean 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;
- (b) “law applicable to guardianship” shall mean, —
  - (i) in relation to 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, the provisions of law contained in

- Rights of Persons with Disabilities Act, 2016 (49 of 2016) and the rules made thereunder; and
- (ii) in relation to 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, the provisions of law of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999) and the rules made thereunder;
- (c) “local level committee” shall mean a 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 (44 of 1999);
- (d) “person with disability” shall mean and include—
- (i) 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; and
- (ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes an individual suffering from severe multiple disability and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions.

**12. Exemptions from certain obligations applicable to processing of personal data of child.** — (1) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child by such class of Data Fiduciaries as are specified in Part A of Fourth Schedule, subject to such conditions as are specified in the said Part.

(2) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child for such purposes as are specified in Part B of Fourth Schedule, subject to such conditions as are specified in the said Part.

**13. Additional obligations of Significant Data Fiduciary.** — (1) A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is notified as such or is included in the class of Data Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the rules made thereunder.

(2) A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit.

(3) A Significant Data Fiduciary shall observe due diligence to verify that technical measures including algorithmic software adopted by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals.

(4) A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government, on the basis of the recommendations of a committee constituted by it, 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.

(5) In this rule, “committee” means a committee constituted by the Central Government for the purpose of this rule, which shall include officials from the Ministry of Electronics and Technology and may include officials from other Ministries or Department of the Central Government.

**14. Rights of Data Principals.** — (1) For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager, shall prominently publish on its website or app, or both, as the case may be, —

- (a) the details of the means using which a Data Principal may make a request for the exercise of such rights; and
- (b) the particulars, if any, such as the username or other identifier of such a Data Principal, which may be required to identify her under its terms of service.

(2) To exercise the rights of the Data Principal under the Act, she may make a request to the Data Fiduciary to whom she has previously given consent for processing of her personal data, using the means and furnishing the particulars required by such Data Fiduciary for the exercise of such rights.

(3) Every Data Fiduciary and Consent Manager shall prominently publish on its website or app, or both, as the case may be, within a reasonable period not exceeding ninety days under its grievance redressal system for responding to the grievances of Data Principals and shall, for ensuring the effectiveness of the system in responding within such period, implement appropriate technical and organisational measures.

(4) To exercise the rights of the Data Principal under the Act, she may, in accordance with the terms of service of the Data Fiduciary and such law as may be applicable, nominate one or more individuals, using the means and furnishing the particulars required by such Data Fiduciary for the exercise of such right.

(5) In this rule, the expression “identifier” shall mean any sequence of characters issued by the Data Fiduciary to identify the Data Principal and includes a customer identification file number, customer acquisition form number, application reference number, enrolment ID, email address, mobile number or licence number that enables such identification.

**15. Transfer of personal data outside the territory of India.**— Any personal data processed by a Data Fiduciary under the Act may be transferred outside the territory of India subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.

**16. Exemption from Act for research, archiving or statistical purposes.** —The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.

**17. Appointment of Chairperson and other Members.**— (1) The Central Government shall constitute a Search-cum-Selection Committee, with the Cabinet Secretary as the chairperson and the Secretaries to the Government of India in charge of the Department of Legal Affairs and the Ministry of Electronics and Information Technology and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as Chairperson.

(2) The Central Government shall constitute a Search-cum-Selection Committee, with the Secretary to the Government of India in the Ministry of Electronics and Information Technology as the chairperson and the Secretary to the Government of India in charge of the Department of Legal Affairs, and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as a Member other than the Chairperson.

(3) The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee, appoint the Chairperson or other Member, as the case may be.

(4) No act or proceeding of the Search-cum-Selection Committee specified in sub-rules (1) and (2) of this rule shall be called in question on the ground merely of the existence of any vacancy or absences in such committee or defect in its constitution.

**18. Salary, allowances and other terms and conditions of service of Chairperson and other Members.**—The Chairperson and every other Member shall receive such salary and allowances and shall have such other terms and conditions of service as are specified in Fifth Schedule.

**19. Procedure for meetings of Board and authentication of its orders, directions and instruments.** —

- (1) The Chairperson shall fix the date, time and place of meetings of the Board, approve the items of agenda therefor, and cause notice specifying the same to be issued under her signature or that of such other individual as the Chairperson may authorise by general or special order in writing.
- (2) Meetings of the Board shall be chaired by the Chairperson and, in her absence, by such other Member as the Members present at the meeting may choose from amongst themselves.
- (3) One-third of the membership of the Board shall be the quorum for its meetings.
- (4) All questions which come up before any meeting of the Board shall be decided by a majority of the votes of Members present and voting, and, in the event of an equality of votes, the Chairperson, or in her absence, the person chairing, shall have a second or casting vote.
- (5) If a Member has an interest in any item of business to be transacted at a meeting of the Board, she shall not participate in or vote on the same and, in such a case, the decision on such item shall be taken by a majority of the votes of other Members present and voting.
- (6) In case an emergent situation warrants immediate action by the Board and it is not feasible to call a meeting of the Board, the Chairperson may, while recording the reasons in writing, take such action as may be necessary, which shall be communicated within seven days to all Members and laid before the Board for ratification at its next meeting.
- (7) If the Chairperson so directs, an item of business or issue which requires decision of the Board may be referred to Members by circulation and such item may be decided with the approval of majority of the Members.

(8) The Chairperson or any Member of the Board, or any individual authorised by it, by a general or special order in writing, may, under her signature, authenticate its order, direction or instrument.

(9) The inquiry by the Board shall be completed within a period of six months from the date of receipt of the intimation, complaint, reference or direction under section 27 of the Act, unless such period is extended by it, for reasons to be recorded in writing, for a further period not exceeding three months at a time.

**20. Functioning of Board as digital office.** — The Board shall function as a digital office, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual.

**21. Terms and conditions of appointment and service of officers and employees of Board.**— (1) The Board may, with previous approval of the Central Government, appoint such officers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of the Act.

(2) The terms and conditions of service of officers and employees of the Board shall be such as are specified in Sixth Schedule.

**22. Appeal to Appellate Tribunal.** — (1) Any person aggrieved by an order or direction of the Board, may prefer an appeal before the Appellate Tribunal, it shall be filed in digital form as the Appellate Tribunal may decide.

(2) An appeal filed with the Appellate Tribunal shall be accompanied by fee of like amount as is applicable in respect of an appeal filed under the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), unless reduced or waived by the Chairperson of the Appellate Tribunal at her discretion, and the same shall be payable digitally using the Unified Payments Interface or such other payment system authorised by the Reserve Bank of India.

(3) The Appellate Tribunal—

(a) shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the provisions of the Act, may regulate its own procedure; and

(b) shall function as a digital office which, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual.

**23. Calling for information from Data Fiduciary or intermediary.** — (1) The Central Government may, for such purposes of the Act as are specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, within the specified period as may be given in such.

(2) Where the disclosure of furnishing of information as referred to in sub-rule (1) is likely to prejudicially affect the sovereignty and integrity of India or security of the State, the Central Government may require the Data Fiduciary or intermediary to not disclose such furnishing to affected Data Principal or any other person except with the previous permission, in writing, of the authorised person.

(3) For the purposes of this rule, the expression “intermediary” shall have the same meaning as assigned to it in the Information Technology Act, 2000 (21 of 2000).

## FIRST SCHEDULE

[See rule 4]

### PART A

#### Conditions for registration of Consent Manager

1. The applicant is a company incorporated in India.
2. The applicant has sufficient capacity, including technical, operational and financial capacity, to fulfil its obligations as a Consent Manager.
3. The financial condition and the general character of management of the applicant are sound.
4. The net worth of the applicant is not less than two crore rupees.
5. The volume of business likely to be available to and the capital structure and earning prospects of the applicant are adequate.
6. The directors, key managerial personnel and senior management of the applicant company are individuals with a general reputation and record of fairness and integrity.
7. The memorandum of association and articles of association of the applicant company contain provisions requiring that the obligations under items 9 and 10 of Part B are adhered to, that policies and procedures are in place to ensure such adherence, and that such provisions may be amended only with the previous approval of the Board.
8. The operations proposed to be undertaken by the applicant are in the interests of Data Principals.
9. It is independently certified that—
  - (a) the interoperable platform of the applicant to enable the Data Principal to give, manage, review and withdraw her consent is consistent with such data protection standards and assurance framework as may be published by the Board on its website from time to time; and
  - (b) appropriate technical and organisational measures are in place to ensure adherence to such standards and framework and effective observance of the obligations under item 11 of Part B.

### PART B

#### Obligations of Consent Manager

1. The Consent Manager shall enable a Data Principal using its platform to give consent to the processing of her personal data by a Data Fiduciary onboarded onto such platform either directly to such Data Fiduciary or through another Data Fiduciary onboarded onto such platform, who maintains such personal data with the consent of that Data Principal.

*Illustration.*

Individuals are enabled to give, manage, review and withdraw their consent to the processing of their personal data through P, a platform maintained by a Consent Manager. X, an individual, is a registered user on P. B1 and B2 are banks onboarded onto P.

*Case 1:* B1 sends a request on P to X for consent to process personal data contained in her bank account statement. X maintains the bank account statement as a digital record in her digital locker. X uses P to directly give her consent to B1, and proceeds to give B1 access to her bank account statement.

*Case 2:* B1 sends a request on P to X for consent to process personal data contained in her bank account statement. X maintains her bank account with B2. X uses P to route her consent through B2 to B1, while also digitally instructing B2 to send her bank account statement to B1. B2 proceeds to send the bank account statement to B1.

2. The Consent Manager shall ensure that the manner of making available the personal data or its sharing is such that the contents thereof are not readable by it.
3. The Consent Manager shall maintain on its platform a record of the following, namely:—
  - (a) Consents given, denied or withdrawn by her;
  - (b) Notices preceding or accompanying requests for consent; and
  - (c) Sharing of her personal data with a transferee Data Fiduciary.
4. The Consent Manager: —
  - (a) shall give the Data Principal using such platform access to such record;
  - (b) shall, on the request of the Data Principal and in accordance with its terms of service, make available to her the information contained in such record, in machine-readable form; and
  - (c) shall maintain such record for at least seven years, or for such longer period as the Data Principal and Consent Manager may agree upon or as may be required by law.
5. The Consent Manager shall develop and maintain a website or app, or both, as the primary means through which a Data Principal may access the services provided by the Consent Manager.
6. The Consent Manager shall not sub-contract or assign the performance of any of its obligations under the Act and these rules.
7. The Consent Manager shall take reasonable security safeguards to prevent personal data breach.
8. The Consent Manager shall act in a fiduciary capacity in relation to the Data Principal.
9. The Consent Manager shall avoid conflict of interest with Data Fiduciaries, including in respect of their promoters and key managerial personnel.
10. The Consent Manager shall have in place measures to ensure that no conflict of interest arises on account of its 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.
11. The Consent Manager shall publish in an easily accessible manner, on its website or app, or both, as the case may be, information regarding: —
  - (a) the promoters, directors, key managerial personnel and senior management of the company registered as Consent Manager;
  - (b) every person who holds shares in excess of two per cent. of the shareholding of the company registered as Consent Manager;

- (c) everybody corporate in whose shareholding any promoter, director, key managerial personnel or senior management of the Consent Manager holds shares in excess of two per cent. as on the first day of the preceding calendar month; and
- (d) such other information as the Board may direct the Consent Manager to disclose in the interests of transparency.

12. The Consent Manager shall have in place effective audit mechanisms to review, monitor, evaluate and report the outcome of such audit to the Board, periodically and on such other occasions as the Board may direct, in respect of—

- (a) technical and organisational controls, systems, procedures and safeguards;
- (b) continued fulfilment of the conditions of registration; and
- (c) adherence to its obligations under the Act and these rules.

13. The control of the company registered as the Consent Manager shall not be transferred by way of sale, merger or otherwise, except with the previous approval of the Board and subject to fulfilment of such conditions as the Board may specify in this behalf.

*Note:* In this Schedule, —

- (a) the expression “body corporate” shall include a company, a body corporate as defined under clause (11) of section 2 of the Companies Act, 2013 (18 of 2013), a firm, a financial institution, a scheduled bank or a public sector enterprise established or constituted by or under any Central Act, Provincial Act or State Act, and any other incorporated association of persons or body of individuals;
- (b) the expressions “company”, “control”, “director” and “key managerial personnel” shall have the same meanings as are respectively assigned to them in the Companies Act, 2013 (18 of 2013);
- (c) the expression “net worth” shall mean the aggregate value of total assets as reduced by the value of liabilities of the Consent Manager as appearing in its books of accounts; and
- (d) the expressions “promoter” and “senior management” shall have the same meanings as are respectively assigned to them in the Companies Act, 2013 (18 or 2013).

## SECOND SCHEDULE

[See rules 5(1) and 16]

### Standards for processing of personal data by State and its instrumentalities under clause (b) of section 7 and for processing of personal data necessary for the purposes specified in clause (b) of sub-section (2) of section 17

Implementation of appropriate technical and organisational measures to ensure effective observance of the following, in accordance with applicable law, for the processing of personal data, namely: —

- (a) Processing is carried out in a lawful manner;
- (b) Processing is done for the uses specified in clause (b) of section 7 of the Act or for the purposes specified in clause (b) of sub-section (2) of section 17 of the Act, as the case may be;
- (c) Processing is limited to such personal data as is necessary for such uses or achieving such purposes, as the case may be;
- (d) Processing is done while making reasonable efforts to ensure the completeness, accuracy and consistency of personal data;

- (e) Personal data is retained till required for such uses or achieving such purposes, as the case may be, or for compliance with any law for the time being in force;
- (f) Reasonable security safeguards to prevent personal data breach to protect personal data in the possession or under control of the Data Fiduciary, including in respect of any processing undertaken by it or on its behalf by a Data Processor;
- (g) Where processing is to be done under clause (b) of section 7 of the Act, the same is undertaken while giving the Data Principal an intimation in respect of the same and—
- (i) giving the business contact information of a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data;
  - (ii) specifying the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may exercise her rights under the Act; and
  - (iii) is carried on in a manner consistent with such other standards as may be applicable to the processing of such personal data under policy issued by the Central Government or any law for the time being in force; and
- (h) 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.

### 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.

		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.

*Note:* In this Schedule, —

- (a) “e-commerce entity” means any person who owns, operates or manages a digital facility or platform for e-commerce as defined in the Consumer Protection Act, 2019 (35 of 2019), but does not include a seller offering her goods or services for sale on a marketplace e-commerce entity as defined in the said Act;
- (b) “online gaming intermediary” means any intermediary who enables the users of its computer resource to access one or more online games;
- (c) “social media intermediary” means an intermediary as defined in clause (w) of sub-rule (1) of rule 2 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; and
- (d) “user”, in relation to—
- (i) an e-commerce entity, means any person who accesses or avails any computer resource of an e-commerce entity; and
- (ii) an online gaming intermediary or a social media intermediary, means any person who accesses or avails of any computer resource of an intermediary for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information.

#### 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

		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.

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

<b>S. No.</b>	<b>Purposes</b>	<b>Conditions</b>
(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.

*Note:* In this Schedule, —

- (a) “advertisement” shall have the same meaning as is assigned to it in the Consumer Protection Act, 2019 (35 of 2019).
- (a) “allied healthcare professional” shall have the same meaning as is assigned to it in the clause (d) of section 2 of the National Commission for Allied and Healthcare Professions Act, 2021 (14 of 2021);
- (b) “clinical establishment” shall have the same meaning as assigned to it in the clause (c) of section 2 of the Clinical Establishments (Registration and Regulation) Act, 2010 (23 of 2010);
- (c) “educational institution” shall mean and include an institution of learning that imparts education, including vocational education;
- (d) “healthcare professional” shall have the same meaning as is assigned to it in clause (j) of section 2 of the National Commission for Allied and Healthcare Professions Act, 2021 (14 of 2021);
- (e) “health services” shall mean the services required to be provided by a healthcare professional as referred to in clause (j) of section 2 of the National Commission for Allied and Healthcare Professions Act, 2021 (14 of 2021); and
- (f) “mental health establishment” shall have the same meaning as is assigned to it in clause (p) of sub-section (1) of section 2 of the Mental Healthcare Act, 2017 (10 of 2017).

## FIFTH SCHEDULE

[See rule 18]

### Terms and conditions of service of Chairperson and other Members

- 1. Salary.** — (1) The Chairperson shall be entitled to receive a consolidated salary of rupees four lakh fifty thousand per month, without the facility of house and car.
- (2) Every Member other than the Chairperson shall be entitled to receive a consolidated salary of rupees four lakh per month, without the facility of house and car.
- 2. Provident Fund.** —The Chairperson and every other Member shall be eligible to contribute to the Provident Fund of the Board, and the manner and terms and conditions applicable in this regard shall, *mutatis mutandis*, be the same as those applicable to other officers and employees of the Board for their Provident Fund.
- 3. Pension and gratuity.** —The Chairperson and every other Member shall not be entitled to payment of pension or gratuity for service rendered in the Board.
- 4. Travelling allowance.**—(1) The Chairperson and every other Member, while on transfer to join the Board, or on the expiry of her term with the Board for proceeding to her home town with family (including in respect of journey undertaken by her and her family), or on tour within India, shall be entitled to journey allowance, daily allowance and reimbursement of expense on transportation of personal effects at such scales and rates as are applicable to an officer of the Central Government in the following level of the pay matrix, namely:—
- (a) level 17, in the case of the Chairperson; and
- (b) level 15, in the case of every other Member.
- (2) The Chairperson and every other Member may undertake tour outside India only in accordance with guidelines or instructions issued by the Central Government, and in respect of such tour, she shall be entitled to draw the same allowances as an officer of the Central Government, in the following level of the pay matrix, is entitled to draw, namely: —
- (a) level 17, in the case of the Chairperson; and
- (b) level 15, in the case of every other Member.
- 5. Medical assistance.** — (1) The Chairperson and every other Member shall be entitled to such medical assistance as may be admissible to them under any group health insurance scheme of the Board for officers and employees of the Board and their eligible dependants.

(2) If the Chairperson or other Member has retired from Government service, or from the service of a public sector entity or a body corporate established by a Central Act, Provincial Act or State Act, and there are a separate set of rules for the grant of medical assistance for such service, she may, in lieu of medical assistance under sub-paragraph (1), opt to be governed by such rules.

**6. Leave.** — (1) The authority competent to sanction leave shall be the Central Government in respect of the Chairperson, and the Chairperson in respect of any other Member.

(2) The Chairperson and every other Member may avail of such kinds of leave as are admissible to a Government servant under sub-clause (i) of clause (a) and clause (b) of sub-rule (1) of rule 26, rules 27, 29, 30 and 40 to 43-C of the Central Civil Services (Leave) Rules, 1972 (hereinafter referred to as “Leave Rules”).

(3) Leave shall be subject to the conditions applicable to a Government servant under rules 7 to 11 and 22 to 25 of the Leave Rules, and the Central Government may, if satisfied that the operation of any of the said rules causes undue hardship in a particular case, by order relax the requirements of that rule to such extent and subject to such exceptions and conditions as it may consider necessary for dealing with the case in a just and equitable manner.

(4) The Chairperson and every other Member shall be entitled to casual leave to such extent as is admissible to a Government servant under instructions issued by the Central Government.

(5) The Chairperson and every other Member shall be entitled to encashment of earned leave standing to her credit, subject to such conditions and in like manner as are applicable to a Government servant under rule 38-A, sub-rules (1) and (2) and sub-clauses (i) and (ii) of clause (a) of sub-rule (6) of rule 39, rule 39-A and rule 39-C of the Leave Rules, subject to the maximum extent of encashment under any of the said rules, other than rule 38-A, being fifty *per cent.* of the earned leave standing to her credit.

**7. Leave travel concession.**—(1) Leave travel concession shall be admissible to the Chairperson and every other Member in accordance with the provisions applicable to persons appointed to civil services and posts in connection with the affairs of the Union of India under rule 3, clauses (a) and (d) of rule 4, rules 5 to 15 and rule 17 of the Central Civil Services (Leave Travel Concession) Rules, 1988, and the entitlement for such concession shall be the same as is applicable to officers of the Central Government in level 17 of the pay matrix in the case of the Chairperson, and to officers of the Central Government in level 15 of the pay matrix in the case of a Member.

(2) The Chairperson and every other Member shall be eligible to avail of either leave travel concession to home town or leave travel concession to any place in India in any period of two years from the date of assumption of their office as a Member.

**8. Other terms and conditions of service.** — (1) The Chairperson and every other Member shall ensure absence of conflict of interest in the performance of the functions of her office and shall not have any such financial or other interests as are likely to prejudicially affect the performance of the functions of such office.

(2) The provisions contained in Part IV to Part IX of the Central Civil Services (Classification, Control and Appeal) Rules, 1965, as applicable to an officer of the Central Government who is a member of a Central Civil Services, Group ‘A’, shall apply, *mutatis mutandis*, to the Chairperson and every other Member.

(3) The Chairperson and every other Member shall not be entitled to any sitting fee for attending meetings of the Board.

(4) The Chairperson and every other Member shall not be entitled to any sumptuary allowance.

(5) Any matter relating to the conditions of service of the Chairperson or any other Member, in respect of which no express provision has been made in these rules, shall be referred to the Central Government for its decision, and the decision of the Central Government on the same shall be final.

**9.** In this Schedule, “pay matrix” shall mean the pay matrix specified in Annexure I to the Central Government’s Resolution published in the Official Gazette *vide* Notification no. 1-2/2016-IC, dated the 25<sup>th</sup> July, 2016.

**SIXTH SCHEDULE**

[See rule 21(2)]

**Terms and conditions of appointment and service of officers and employees of Board**

**1. Classes of officials.** — (1) The Board may, in accordance with the Fundamental Rules and applicable guidelines issued by the Ministry of Personnel, Public Grievances and Pensions, Department of Personnel and Training, appoint officers and employees on deputation from the Central Government, a State Government, an autonomous body under the overall control of the Central Government or a State Government, a statutory body, or a public sector enterprise, for a period not exceeding five years.

(2) The Board may also receive or take on deputation any officer or other employee from the National Institute for Smart Government, for a period not exceeding five years, with salary and allowances guided by market standards and on such other terms and conditions as the Board may decide.

**2. Gratuity.** —The officers and employees shall be entitled to payment of such gratuity as may be admissible under the Payment of Gratuity Act, 1972 (39 of 1972).

**3. Travelling allowance.** —The travelling allowance payable to the officers and employees shall, *mutatis mutandis*, be the same as those applicable to the officers and employees of the Central Government.

**4. Medical assistance.** —The officers and employees shall be entitled to such medical assistance as may be admissible to them and their eligible dependants under any group health insurance scheme of the Board, made with the previous approval of the Central Government.

**5. Leave.** — (1) The officers and employees may avail of such kinds of leaves as are admissible to a Government servant under the Central Civil Services (Leave) Rules, 1972, subject to the conditions applicable under the said rules, and shall be eligible for encashment of earned leave as provided therein.

(2) The officers and employees shall be entitled to casual leave to such extent as is admissible to a Government servant under instructions issued by the Central Government.

**6. Leave travel concession.** — Leave travel concession shall be admissible to the officers and employees appointed under clause (1) of paragraph 1, in accordance with the provisions applicable to persons appointed to civil services and posts in connection with the affairs of the Union of India under the Central Civil Services (Leave Travel Concession) Rules, 1988.

**7. Other terms and conditions of service.** — (1) The provisions of the Civil Service (Conduct) Rules, 1964 shall apply to the officers and employees in like manner as applicable to a person appointed to a civil service or post in connection with the affairs of the Union of India under the said rules.

(2) The provisions contained in Part IV to Part IX of the Central Civil Services (Classification, Control and Appeal) Rules, 1965 shall apply, *mutatis mutandis*, to the officers and employees appointed under clause (1) of paragraph 1, in like manner as applicable to a Government servant under the said rules.

(3) Any matter relating to the terms and conditions of service of the officers and employees appointed under clause (1) of paragraph 1, in respect of which no express provision has been made in these rules, shall be referred to the Central Government for its decision, and the decision of the Central Government on the same shall be final.

**SEVENTH SCHEDULE**

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

<b>S. no.</b>	<b>Purpose</b>	<b>Authorised person</b>
(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.

[F. No. AA-11038/1/2025-CLandES]

AJIT KUMAR, Jt. Secy.



The Digital Personal Data Protection Act, 2023, (hereinafter referred to as “DPDP Act”) as well as Rules 17 and 23(2) of The Digital Personal Data Protection Rules, 2025, are *ultra vires* the Constitution, and other consequential reliefs.

2. That the Petitioner craves leave to rely on the contents of the accompanying petition for the purposes of the present application, which are not being reproduced herein for the sake of brevity.
3. That Section 44(3) of the DPDP Act, which amends Section 8(1)(j) of the RTI Act, has been brought into force immediately on 13.11.2025 vide publication of GSR 843(E) in the Official Gazette. As such, the balancing provisions inherent in the unamended Section 8(1)(j) of RTI Act stand immediately deleted, thereby significantly curtailing the citizens’ right to information and right to know about public functionaries entrusted with public functions and duties. This is a heavy blow to ideas of transparency and open governance, and is a legislative act which directly interferes with the fundamental rights under Articles 19(1)(a) and 21, and violates various judgments of this Hon’ble Court including the Constitution Bench dicta in *KS Puttaswamy vs Union of India* (2019) 1 SCC 1, which holds that larger public interest must prevail over the right to privacy.
4. That the Petitioner submits that the amendment introduced through Section 44(3) is ex-facie unconstitutional, as privacy is not a permissible ground for restrictions under Article 19(2). Further, while the amendment

is effectuated through an Act limited in scope to “digital personal data”, it has amended Section 8(1)(j) of RTI Act for digital as well as non digital data, which is impermissible and commits violence upon the statutory architecture of the RTI law. The unamended provision has been in vogue for over twenty years, and this Hon’ble Court in various judgments has emphasized the importance for disclosure of data in terms of Section 4(1)(b) of the RTI Act, which now stands abridged by introduction of Section 44(3) of DPDP Act. As such, no harm will result from staying the operation of the amendment to Section 8(1)(j) of RTI Act, and restoring status quo prior to enactment of Section 44(3) DPDP Act, during the pendency of the captioned proceedings.

5. That the present application is bonafide and in the interest of justice, causing no prejudice to any party whatsoever.

### **PRAYER**

In light of the facts and circumstances stated hereinabove, it is most humbly prayed that this Hon’ble Court may be pleased to:

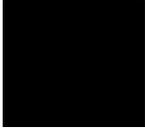
- A.** Direct that the operation of Section 44(3) of The Digital Personal Data Protection Act, 2023, shall be stayed during the pendency of the captioned proceeding; and

**B.** Pass any other order as this Hon'ble Court may deem fit and necessary.

AND FOR THIS ACT OF KINDNESS THE APPLICANT  
SHALL AS IN DUTY BOUND FOREVER PRAY

PETITIONER/APPLICANT

Through:

  
**AAKARSH KAMRA**  
**ADVOCATE ON RECORD**  
**AOR CODE: 2599**

**SETTLED BY: VRINDA GROVER, ADV**

**DRAFTED BY: SOUTIK BANERJEE, ADV**  
**DEVIKA TULSIANI, ADV**







