AS INTRODUCED IN THE RAJYA SABHA
ON THE 5TH DECEMBER, 2025

**Bill No. XXXVIII of 2025**

# THE DIGITAL PERSONAL DATA PROTECTION (AMENDMENT) BILL, 2025

A

BILL

*to amend the Digital Personal Data Protection Act, 2023.*

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

Short title and commencement.

**1.** *(1)* This Act may be called the Digital Personal Data Protection (Amendment) Act, 2025.

*(2)* It shall come into force at once.

Amendment of section 2.

**2.** In the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the principal Act), in section 2, — 22 of 2023.

*(i)* after clause *(o)*, the following new clause shall be inserted, namely,—

"(*oa*): 'harm' includes, but is not limited to:

*(i)* bodily or mental injury;

*(ii)* loss, distortion or theft of identity;

*(iii)* loss of reputation or humiliation;

*(iv)* loss of employment;

*(v)* discriminatory treatment;

*(vi)* financial loss, or damage or loss of property;

*(vii)* subjection to blackmail or extortion;

*(viii)* denial or withdrawal of a service, benefit or goods resulting from an evaluative decision about the Data Principal;

*(ix)* observation or surveillance not reasonably expected by the Data Principal;

*(x)* movement or any other action arising out of fear of being observed or surveilled; *(xi)* psychological manipulation which impairs the autonomy of the individual;

*(xii)* any restriction placed or suffered directly or indirectly on speech; and

*(xiii)* unauthorized profiling."

*(ii)* after clause (*x*), the following *new* clauses shall be inserted, namely,—

"*(xa)* "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal;

*(xb)* "reasonable security safeguards" includes, but is not limited to, —

*(i)* implementation of such security practices and standards and having a comprehensive, documented information security programme and policies containing managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business:

Provided that in the event of an information security breach, the Data Fiduciary or the Data Processor, as the case may be, shall be required to demonstrate that they have implemented security control measures as per their documented information security programme and information security policies;

*(ii)* adherence to the international Standard IS/ISO/IEC 27001 on 'Information Technology - Security Techniques — Information Security Management Systems – Requirements':

Provided that any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC

codes of best practices for data protection, as per sub-clause (*i*), shall get its codes of best practices duly approved and notified by the Board for effective implementation:

Provided further that the body corporate or a person on its behalf, who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection, as approved and notified by the Board, shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through an independent auditor, duly approved by the Board, at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource, whichever is earlier; and

*(iii)* such other additional safeguards as may be prescribed under sub-section *(5A)* of section 8."

**3.** In section 3 of the principal Act, in clause *(b)*, after the words "connection with", the words "or profiling of," shall be inserted. Amendment of section 3.

**4.** In section 6 of the principal Act, after sub-section *(10)*, the following new sub-sections shall be inserted, namely:— Amendment of section 6.

"(*11*) Notwithstanding anything contained in this Act, no Data Fiduciary shall share the personal data of a Data Principal with any other Data Fiduciary or Data Processor unless -

*(a)* specific, prior, informed and explicit consent is obtained for such data sharing, and

*(b)* the purpose of such sharing is disclosed at the time of seeking such consent.

Provided that where personal data is proposed to be transferred to a foreign country, the Data Principal shall be informed of such eventuality in advance.

(*12*) The consent under sub-section *(11)* shall be obtained independently of any general consent for processing any other personal data obtained previously.

(*13*) Any sharing of data in contravention of sub-sections *(11)* and *(12)* shall be deemed to be personal data breach and shall attract the same penalty, as provided for non-compliance of the obligation under sub-section (5) of section 8 and also the liability to compensate the Data Principal, as provided under section 6A.

*Explanation.*— For the purposes of this section, "sharing" includes any transfer, transmission, dissemination, disclosure, or making available of personal data by one Data Fiduciary to another or to a Data Processor, whether electronically or otherwise."

**5.** After section 6 of the principal Act, the following new section shall be inserted, namely:— Insertion of new section 6A.

"**6A.** *(1)* A Data Principal shall have the right to seek compensation for any harm suffered due to contravention of the provisions of this Act by a Data Fiduciary or a Data Processor. Right to Compensation.

*(2)* The Board shall have the power to adjudicate and award compensation, commensurate with the harm caused."

**6.** In section 7 of the principal Act, —

Amendment of section 7.

*(i)* after clause *(e)*, the following proviso shall be inserted, namely;—

"Provided that the compliance of foreign judgment or order shall be subject to compliance, through courts of competent jurisdiction in India, with sections 13,14 and 44A read with sub-sections *(5)* and *(6)* of section 2 of the Code of Civil Procedure, 1908.";

5 of 1908.

*(ii) a*fter clause (*i*), the following new clauses shall be inserted, namely:

"(*j*) any exemption granted under this section shall be reasonable, not excessive or arbitrary, and shall be subject to judicial review; and

(*k*) notwithstanding anything contained in this section, no data shall be processed for profiling, behavioural monitoring or targeted advertising without the explicit and informed consent of the Data Principal."

Amendment of section 8.

**7.** In section 8 of the principal Act, **—**

*(i)* in sub-section *(4)*, after the words "A Data Fiduciary", the words "or a Data Processor engaged, appointed, used or otherwise involved by a Data Fiduciary on its behalf", shall be inserted;

*(ii)* after sub-section *(5)*, the following new sub-section shall be inserted, namely,—

"*(5A)* Save as provided in clause (*xb*) of section 2, the Central Government shall, within three months from the date on which the provisions of this Act come into force, prescribe by rules, additional reasonable security safeguards to be followed by a Data Fiduciary and Data Processor:

Provided that the rules so framed shall be congruent with clause (*xb*) of section 2 and the rules framed by the Central Government under clause (*ob*) of sub-section *(2)* of section 87 read with section 43A of the Information Technology Act, 2000.";

21 of 2000.

*(iii)* in sub-section *(6)*, after the words "the Data Fiduciary", the words "or the Data Processor, as the case may be," shall be inserted.

Insertion of new section 8A.

**8.** After section 8 of the principal act, the following new section shall be inserted, namely:—

Right to be Forgotten.

"**8A.** *(1)* Notwithstanding anything contained in this Act, a Data Principal shall have the right to request the erasure, deletion, or restriction on continued retention or disclosure of her personal data held by the Central Government, State Government, or any of their instrumentalities, where –

*(a)* the data is no longer necessary for the purpose for which it was collected or processed by the authority;

*(b)* the Data Principal has withdrawn consent, and there is no legal ground for retention; or

*(c)* retention of such data is not necessary for compliance with a legal obligation or for a task carried out in public interest.

*(2)* Every such request made under sub-section (*1*) shall be duly considered by the concerned public authority, and if found valid, the authority shall —

*(a)* erase or anonymize the relevant data; and

*(b)* confirm such erasure or anonymization in writing to the Data Principal within thirty days of receipt of the request.

*(3)* Any refusal to act on a request received under sub-section (*1*) shall be intimated to the Data Principal within thirty days of the receipt of such request and shall be accompanied by written reasons, and the Data Principal shall have the right to appeal against such refusal before the Board."

**9.** In section 9 of the Principal Act, sub-sections *(4)* and *(5)* shall be omitted. Amendment of section 9.

**10.** In section 11 of the Principal Act, after sub-section *(1)*, the following new sub-section shall be inserted, namely;— Amendment of section 11.

"(*1A*) The Data Principal shall have the right to make a demand to the Data Fiduciary, to whom she has previously given consent and where the processing has been carried out through automated means, to transfer her personal data to another Data Fiduciary of her choice".

**11.** In section 17 of the Principal Act, - Amendment of section 17.

*(i)* sub-section *(3)*, including the Explanation thereto, shall be omitted;

*(ii)* for sub-section *(5)*, the following shall be substituted, namely:—

"(*5*) Any exemption or relaxation under this section shall be reasonable, not excessive or arbitrary, and shall be subject to judicial review.";

*(iii)* after sub-section *(5)*, the following new sub-section shall be inserted, namely:—

"(*6*) The provisions contained in section 6 of the Act pertaining to the conferring of consent by a Data Principal for the processing of personal data shall apply *mutatis mutandis* to the processing of personal data under this section unless expressly excluded by law or rules."

**12.** In section 19 of the principal Act,— Amendment of section 19.

*(i)* for sub-section *(2)*, the following shall be substituted, namely:—

"*(2)* The Chairperson and Members of the Board shall be appointed by a Selection Committee comprising:

*(a)* the Chief Justice of India or a Judge of the Supreme Court nominated by him – Chairperson *ex-officio*;

*(b)* the Leader of the Opposition in the House of the People – Member *ex-officio*;

*(c)* the Minister in-charge of the Union Ministry of Electronics and Information Technology – Member *ex-officio*;

*(d)* the Attorney General of India – Member *ex-officio*; and

*(e)* an independent expert with vast experience in the field of Data Protection, Information Technology, Data Management, Data Science, Data Security or Cyber and internet Laws, to be nominated by the Chairman of the Council of the States in such manner as may be prescribed- Member:

Provided that the Selection Committee may co-opt one Director each from any of the Indian Institutes of Technology and Indian Institutes of Management as subject experts without having the right to vote in the proceedings thereof.

*Explanation*.— For the purpose of removal of doubts, it is hereby declared that where the Leader of the Opposition in the House of the People has not been recognised as such, the leader of the single largest party in opposition to the Government in the House of the People shall deemed to be the Leader of the Opposition."

*(ii)* after sub-section *(2)*, the following new sub-section shall be inserted, namely,—

"*(2A)* The Board shall be an independent statutory authority and shall not be subject to the directions of the Central Government in the discharge of its functions."

Amendment of section 22.

**13.** In section 22 of the principal Act, in sub-section *(3)*, the words "except with the previous approval of the Central Government", shall be deleted.

Amendment of section 23.

**14.** In section 23 of the principal Act, for sub-section *(1)*, the following shall be substituted, namely:—

"*(1)* The Board shall regulate and observe its own procedure in regard to the holding or and transaction of business at its meetings, including by digital means, and authenticate its orders, directions and instruments, in accordance with the regulations, that may be issued by the Board in this regard, from time to time."

Amendment of section 24.

**15.** In section 24 of the principal Act, the words, "with previous approval of the Central Government,", shall be deleted.

Amendment of section 32.

**16.** In section 32 of the principal Act, ;—

*(i)* for sub-section *(4)*, the following shall be substituted, namely:

"(*4*) A voluntary undertaking shall not absolve a Data Fiduciary or a Data Processor, as the case may be, from liability to pay compensation under section 6A, nor bar adjudication under section 33."

*(ii)* sub-section (*5*) shall be omitted.

Amendment of section 33.

**17.** In section 33 of the principal Act, after sub-section *(1)*, the following new sub-section shall be inserted, namely:

"*(1A)* In the eventuality of imposing penalty under sub-section *(1)*, the Board shall also determine and award compensation to the affected Data Principal having regard to the gravity of the harm, nature of the breach, and extent of infringement of rights."

Amendment of section 40.

**18.** In section 40 of the principal Act, in sub-section *(2)*, clause *(t)* shall be omitted.

Amendment of section 44.

**19.** In section 44 of the principal Act,—

*(i)* in sub-section (2), clauses *(a)* and *(c)*, shall be omitted.

*(ii)* sub-section (*3*) shall be omitted.

## STATEMENT OF OBJECTS AND REASONS

In the digital age, personal data has emerged as a critical asset with wide-ranging implications for individual rights and privacy. The Digital Personal Data Protection Act, 2023 was enacted with the stated objective of safeguarding personal data and regulating its processing. However, a closer scrutiny of the Act reveals significant shortcomings that may undermine the very rights it purports to protect.

Grave concerns have been raised regarding the structure and independence of the Data Protection Board, the principal adjudicatory authority under the Act. The current provision empowers the Central Government to appoint the Chairperson and Members of the Board without laying down any criteria or requiring a transparent selection process. Earlier, the Joint Parliamentary Committee had recommended an independent regulatory framework.

In addition to the issues of independence and transparency in the constitution of the Data Protection Board, section 22(3) of the Act permits the Central Government to waive the mandatory one-year cooling-off period for the Chairperson or any Member of the Board before they accept any re-employment. This discretionary power, if left unchecked, risks compromising the integrity and impartiality of the Board. It creates a fertile ground for conflicts of interest and post-retirement inducements that could distort regulatory outcomes and weaken public trust in the adjudicatory body. The cooling-off period must be treated as an absolute bar, without exceptions, to ensure that Members and the Chairperson of the Board remain free from undue influence during and after their term of office.

The introduction of the concept of ‘voluntary undertaking’ under section 32 allows entities in violation of the law to submit undertakings and thereby avoid formal inquiry and penalties. This provision creates a potential escape route for powerful Data Fiduciaries and erodes the deterrent effect of the law. Compounding this, the Act is silent on compensatory relief to Data Principals who have suffered harm. There is a need to incorporate the global best practices, such as the European Union's General Data Protection Regulation (GDPR), in the Act to recognize the right to claim compensation by the Data Principal - thus offering redressal for privacy violations or data breaches.

Further, the Act introduces the notion of “reasonable security safeguards” as a compliance obligation for data fiduciaries but does not define or prescribe minimum standards for such safeguards. This ambiguity fosters compliance in form rather than in substance. The Act simultaneously repeals Section 43A and clause (ob) of sub-section (2) of Section 87 of the Information Technology Act, 2000 - provisions that had enabled affected individuals to seek compensation for negligence in data protection.

Likewise, the extensive exemption powers under Section 17 vest the Central Government with authority to exempt public and private entities, including start-ups, from complying with the provisions of the Act. The Act also does not guarantee rights such as the "right to be forgotten" in relation to data held by the State.

The legislation also affects the Right to Information Act, 2005 by effectively overriding Section 8(1)(j) of the RTI Act through section 44(3), and there is a likelihood of the provision being misused to withhold information merely on the ground that it constitutes personal data, even in cases where its disclosure will serve larger public interest or where such information could not ordinarily be denied to Parliament or a State Legislature.

Other deficiencies in the Act include the exclusion of provisions requiring Data Fiduciaries to obtain specific consent before sharing data with

third parties or foreign entities; exclusion of Data Processors from the ambit of responsibility under the Act; and the lack of provisions for the right to data portability, despite these being recommended by earlier drafts or Parliamentary Committees.

Crucially, children's data, despite being nominally protected under Section 9, is subject to broad governmental exemptions. Such exemptions allow for behavioural monitoring, profiling, and targeted advertising directed at children without robust parental consent mechanisms, which might undermine child safety and contradicts the protective intent of the law.

Moreover, there are apprehensions that the Act fails to rein in state surveillance effectively. Clauses such as Sections *7(b)* and *7(c)* allow the processing of personal data for vaguely defined state functions and national security, without explicit consent. Section 7(e) permits the enforcement of foreign civil and contractual judgments without the oversight of Indian courts—sidestepping safeguards under the Code of Civil Procedure, 1908.

The concept of "harm" to Data Principals, a foundational element in previous iterations of the Data Protection Bill, has been conspicuously omitted in the Act. As a result, there is no established basis for individuals to claim compensation or for regulators to evaluate the impact of privacy violations.

In light of these substantial gaps, this Amendment Bill seeks to:—

1. Define "harm" and "profiling" and recognize the right to claim compensation for damages resulting from breaches;

2. Establish minimum standards for reasonable security safeguards and reinstate repealed protective provisions from the Information Technology Act, 2000;

3. Mandate specific, informed, and unbundled consent for data sharing, including cross-border transfers;

4. Ensure the independence of the Data Protection Board;

5. Introduce the right to data portability, and require accountability from data processors as well as fiduciaries;

6. Eliminate arbitrary exemptions, particularly those allowing the State to operate outside the framework of the Act;

7. Ensure judicial review and transparency in all exemptions and governmental decisions under the Act;

8. Protect children's data more rigorously by disallowing exemptions for profiling, monitoring, or advertising without consent;

9. Reinstate the original provisions of the Right to Information Act, 2005, ensuring India's transparency framework and the foundational principles of democratic accountability; and

10. Provide for such other matters connected therewith or incidental thereto.

The objective of this proposed legislation is not only to fill legislative gaps but also to reorient the Digital Personal Data Protection Act, 2023 toward its stated goal of protecting the fundamental right to privacy as enshrined under Article 21 of the Constitution of India. The Supreme Court, in Justice K.S Puttaswamy (Retd.) *v.* Union of India and *Ors.*, has recognized that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution". It is the solemn duty of the legislature to give effect to this principle in both letter and spirit.

This Bill, therefore, seeks to reclaim the balance between innovation and individual rights, governance and accountability, regulation and freedom– while laying the foundation for a data protection regime that truly honours constitutional values and public trust.

The Bill seeks to achieve the aforesaid objectives.

JOHN BRITTAS.

*ANNEXURE*

EXTRACTS FROM THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

(22 OF 2023)

* * * * *

**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;

* * * * *

**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 the following uses, namely:—

* * * * *

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

General obligations of Data Fiduciary.

**8.** * * * * *

(*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.

* * * * *

(*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.

* * * * *

**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. Processing of personal data of children.

*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.

* * * * *

**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.

* * * * *

**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.

* * * * *

(*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.

* * * * *

*(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.

* * * * *

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.

* * * * *

Resignation by Members and filling of vacancy.

**22.** * * * * *

*(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.

Proceedings of the Board.

**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.

* * * * *

Officers and employees of the Board.

**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.

* * * * *

Voluntary undertaking.

**32.** * * * * *

(*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.

* * * * *

Power to make rules.

**40.** *(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:—

* * * * *

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

* * * * *

**44.** * * * * * Amendment to certain Acts.

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

*(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;".

* * * * *

RAJYA SABHA

A

BILL

to amend the Digital Personal Data Protection Act, 2023.

*(Dr. John Brittas, M.P.)*

RS-P&PS—PMB(E)—319— 08.12.2025