AS INTRODUCED IN THE RAJYA SABHA
ON THE 7TH FEBRUARY, 2025

Bill No. LXV of 2024

THE DIGITAL PERSONAL DATA PROTECTION (AMENDMENT) BILL, 2024

A

BILL

to amend the Digital Personal Data Protection Act, 2023.

BE it enacted by Parliament in the Seventy-fifth 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, 2024.

(2) It shall come into force at once.

Amendment of section 2.

22 of 2023.

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

(i) for clause *(i)*, the following shall be substituted, namely:-

'*(i)* "Data Fiduciary" means any person including a State, a company, a non-governmental organisation, juristic entity or any individual, who alone or in conjunction with other persons determines the purpose and means of collection, storage, disclosure, sharing or processing of personal data;';

(ii) for clause *(k)*, the following shall be substituted, namely:-

'(*k*) "Data Processor" means any person including a State, a company, a non-governmental organisation, juristic entity or any individual, who processes personal data on behalf of a Data Fiduciary;';

(iii) after clause *(x)*, the following new clause shall be inserted, namely:-

'(*xa*) "sensitive personal data" means such personal data, which may reveal, be related to, or constitute financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, or any other data which may be categorised as such, from time to time, by the Central Government.

Explanation— For the purposes of this clause, the expressions,-

(a) "financial data" means personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or regarding the relationship between a financial institution and a data principal including financial status and credit history;

(b) "health data" means personal data related to the past, present or future physical or mental health state of the data principal, data collected in the course of registration for or provision of health services and any data associated with the data principal for the provision of specified health services;

(c) "official identifier" means any number, code or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of such data principal;

(d) "biometric data" means facial images, fingerprints, iris scans or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person;

(e) "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the behavioural characteristics, physiology or the health of that natural person and which results, in particular, from an analysis of a biological sample from the natural person in question;

(f) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy or any other similar medical procedure; and

(g) "intersex status" means the condition of a data principal who is a combination of female and male; or neither wholly female nor wholly male; or neither female nor male;';

(iv) after clause *(z)*, the following new clause shall be inserted, namely:-

'(za)"significant harm" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm.

Explanation: For the purposes of this clause, "harm" includes bodily or mental injury; loss, distortion or theft of identity; financial loss or loss of property; loss of reputation or humiliation; loss of employment; any discriminatory treatment; any subjection to blackmail or extortion; any denial or withdrawal of a service, benefit or goods resulting from an evaluative decision about the data principal; any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or being under surveillance; any observation or surveillance that is not reasonably expected by the data principal; psychological manipulation which impairs the autonomy of the data principal; or such other harm, as may be prescribed.'; and

(v) the clauses *(za)* and *(zb)* may accordingly be re-numbered as *(zb)* and *(zc)* respectively.

Amendment of section 3.

3. In the principal Act, in section 3, in clause *(a)*, after the words "where personal data is collected", the words "stored, disclosed, shared or otherwise processed", shall be inserted.

Amendment of section 4.

4. In the principal Act, in section 4, in sub-section *(1)*-

(i) for clause *(a)*, the following shall be substituted, namely:-

'*(a)* only for the specific purpose for which the Data Principal has given her consent and which the Data Principal would reasonably expect that such personal data shall be only used for such purpose and in the context and circumstances in which the personal data was collected; or'

(*ii*) the following proviso shall be inserted, namely:-

"Provided that the processing of such data shall be in a fair and reasonable manner ensuring the privacy of the Data Principal."

Insertion of new section 4A.

5. In the principal Act, after section 4, the following new section shall be inserted, namely:-

Limitation on collection of personal data.

"**4A**. The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data."

Amendment of section 5.

6. In the principal Act, in section 5, in sub-section *(1)*-

(i) after the words "under section 6 for consent", the words "at the time of collection of personal data", shall be inserted;

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

"*(ia)* the source of collection, if the personal data is not collected directly from the Data Principal;

(ib) the individuals or entities including other Data Fiduciaries or Data Processors, with whom such personal data may be shared, if applicable;

(ic) the period for which personal data shall be retained or where

such period is not known, the criteria for determining such period;"

Insertion of new section 5A.

7. In the principal Act, after section 5, the following new section shall be inserted namely:-

Categorisation of personal data as sensitive personal data.

"**5A**. *(1)* The Central Government shall, from time to time, notify such categories of personal data as "sensitive personal data", having regard to—

(a) the risk of significant harm that may be caused to the Data Principal by the processing of such category of personal data;

(b) the expectation of confidentiality attached to such category of personal data;

(c) whether a significantly discernible class of Data Principals may suffer significant harm from the processing of such category of personal data; and

(d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

(2) The Central Government may also specify, by rules and regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data."

Amendment of section 6.

8. In the principal Act, in section 6,

(i) after sub-section *(1),* the following new sub-section shall be inserted, namely:-

"*(1A)* The consent of the Data Principal in respect of processing of any sensitive personal data shall be explicitly obtained—

(a) after informing her the purpose of, or operation in, processing which is likely to cause significant harm to the Data Principal;

(b) in clear terms without recourse to inference from conduct in a context; and

(c) after giving her the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing."

(ii) in sub-section *(6),* for the words "within a reasonable time", the words "within a period of thirty days from the date of withdrawal of consent", shall be substituted.

(iii) after sub-section *(7),* the following new sub-sections shall be inserted:-

"*(7A)* The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

(7B) The burden of proof that the consent has been given by the Data Principal for processing of the personal data under this section shall be on the Data Fiduciary."

9. In the principal Act, in section 7, for clause *(a)*, the following shall be substituted:- Amendment of section 7.

"*(a)* only for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary."

10. In the principal Act, after section 7, the following new section shall be inserted, namely:- Insertion of new section 7A.

Restriction on retention of personal data.

"**7A.***(1)* The Data Fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is collected and processed and shall delete the same at the end of such period.

(2) Notwithstanding anything contained in sub-section *(1)*, the personal data may be retained for a longer period only if explicitly consented to by the Data Principal or is necessary to comply with any obligation under any law for the time being in force.

(3) The Data Fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession.

(4) Where it is not necessary for personal data to be retained by the Data Fiduciary under sub-section *(1)* or sub-section *(2)*, then, such personal data shall be deleted in such manner as may be specified by regulations."

11. In the principal Act, in section 8, in sub-section *(7)*, for clause *(a)*, the following shall be substituted, namely:- Amendment of section 8.

"*(a)* erase personal data, upon the Data Principal withdrawing her consent or immediately upon the specified purpose for which the personal data was collected or processed has been served."

12. In the principal Act, in section 12, after sub-section *(3)*, the following new sub-sections shall be inserted, namely:- Amendment of section 12.

"*(4)* Where the Data Fiduciary receives a request under sub-sections *(2)* and *(3)*, and the Data Fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such Data Fiduciary shall provide the Data Principal with adequate justification in writing for rejecting the application, within a period of thirty days of receipt of such request.

(5) Where the Data Principal is not satisfied with the justification provided by the Data Fiduciary under sub-section *(4)*, the Data Principal may require that the Data Fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the Data Principal.

(6) Where the Data Fiduciary corrects, completes, updates or erases any personal data in accordance with sub-sections *(2)* and *(3)*, such Data Fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the Data Principal or on decisions made regarding them."

Insertion of new section 12A and 12B.

13. In the principal Act, after section 12, the following new sections shall be inserted, namely:-

Right to data portability.

"**12A.** *(1)* Where the processing has been carried out through automated means, the Data Principal shall have the right to—

(a) receive the following personal data in a structured, commonly used and machine-readable format—

(i) the personal data provided to the Data Fiduciary;

(ii) the data which has been generated in the course of provision of services or use of goods by the Data Fiduciary; or

(iii) the data which forms part of any profile on the Data Principal, or which the Data Fiduciary has otherwise obtained; and

(b) transfer the personal data referred to in clause (a) to any other Data Fiduciary in the format referred to in that clause.

(2) The provisions of sub-section *(1)* shall not apply where—

(a) processing is necessary for functions of the State or in compliance of any law or any judgement or order of any court, quasi-judicial authority or tribunal under section 7;

(b) compliance with the request in sub-section (1) would not be technically feasible, as determined by the Data Fiduciary in such manner as may be specified by regulations.

Right to be forgotten.

12B. *(1)* The Data Principal shall have the right to restrict or prevent the continuing disclosure of her personal data by a Data Fiduciary where such processing or disclosure—

(a) has served the purpose for which it was collected or is no longer necessary for the purpose and there are no other legal grounds for its processing or disclosure; or

(b) was made with the consent of the Data Principal under section 6 and such consent has since been withdrawn; or

(c) has been objected to by the Data Principal and there are no overriding legitimate grounds for processing or disclosure; or

(d) was made contrary to the provisions of this Act or any other law for the time being in force.

(2) The rights under sub-section *(1)* may be enforced only on an order of the Board made on an application filed by the Data Principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses *(a), (b)* or clause *(c)* of that sub-section:

Provided that no order shall be made under this sub-section unless it is shown by the Data Principal that her right or interest in preventing or restricting the continued disclosure of her personal data overrides the right to freedom of speech and expression and the right to information of any other citizen.

(3) The Board shall, while making an order under sub-section *(2)*,have regard to—

(a) the sensitivity of the personal data;

(b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented;

(c) the role of the Data Principal in public life;

(d) the relevance of the personal data to the public; and

(e) the nature of the disclosure and of the activities of the Data Fiduciary, particularly whether the Data Fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.

(4) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Board under sub-section *(2)*, does not satisfy the conditions referred to in that sub-section, he may apply for the review of that order to the Board in such manner as may be prescribed, and the Board shall review the order.

(5) Any person aggrieved by an order made under this section by the Board may prefer an appeal to the Appellate Tribunal.

14. In the principal Act, in section 13, in sub-section *(2)*, for the words "within such period as may be prescribed", the words "within thirty days", shall be substituted. Amendment of section 13.

15. In the principal Act, in section 17, sub-section *(3)* may be omitted. Amendment of section 17.

16. In the principal Act, in section 20, for sub-section*(2)*, the following shall be substituted, namely: - Amendment of section 20.

"*(2)* The Chairperson and other Members shall hold office for a term of five years and shall not be eligible for re-appointment."

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

STATEMENT OF OBJECTS AND REASONS

In a country like India with a population of around 1.4 billion, out of which at least 1.2 billion are mobile phone users, the State has an onerous responsibility to ensure data privacy of citizens, particularly of personal data. At a time when technology has become the defining paradigm, particularly in the post-COVID world, which represents a watershed moment for the role of digital technologies in our lives, data is the new 'gold', a very valuable asset, which if processed and used wisely can be a gamechanger in the development story of any society and nation. Data is the lifeblood of the digital economy. In this scenario, putting in place a strong data privacy regime has become a necessity of the times to leverage the potential of data without compromising the privacy of its citizens. Protection of personal data holds the key to empowerment, progress, and innovation.

The Right to Privacy was not directly envisaged by the Constitution makers and as such does not find a mention in Part III of the Constitution relating to Fundamental Rights. However, through various judgements over the years the Courts of the country have interpreted the other rights in the Constitution to be giving rise to a limited right to privacy – primarily through Article 21 – the right to life and liberty. In 2015, this interpretation was challenged and referred to a larger Bench of the Supreme Court in the writ petition of Justice K.S Puttaswamy & Another vs. Union of India and Others [Writ Petition (civil) No. 494 of 2012]. The Court in a landmark judgement on 24 August, 2017 unanimously ruled that privacy is a fundamental right, and that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, as a part of the freedoms guaranteed by Part III of the Constitution. The Bench also ruled that the right to privacy is not absolute, but is subject to reasonable restrictions, as is every other fundamental right.

Privacy enjoys a robust legal framework internationally. Article 12 of the Universal Declaration of Human Rights, 1948 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966, legally protect persons against "arbitrary interference" with one's privacy, family, home, correspondence, honour and reputation. The General Data Protection Regulation (GDPR) of the European Union, which came into force on 25 May 2018 is also a case in point.

The Digital Personal Data Protection (DPDP) Act passed in 2023 (22 of 2023) is a welcome step in this direction. However, there are many shortcomings and loopholes in the new Act, which waters down the legislative intent of ensuring a strong data privacy framework at par with other nations and dilutes accountability and transparency. As a corrective measure to the Act, this Bill aims to widen its scope by addressing certain key aspects and concerns flagged by stakeholders. To begin with, the applicability of the Act is proposed to be made broad based to include not only personal data that is collected, but also stored, disclosed, shared or otherwise processed. Certain definitions are also being proposed to render clarity to the various terminologies used in the Bill. Purpose limitation has been proposed to ensure that data may be processed only for the specific purpose for which the Data Principal has given consent and shall be used only in the context and circumstances in which the data was collected, thus guaranteeing the right to privacy to all citizens. The scope of the information to be accompanied or preceded by the notice to be given by a Data Fiduciary to a Data Principal at the time of collection of personal data has also been widened so that each individual while giving their consent can

make an informed and free decision with full knowledge of the implications of giving consent.

The present Act is silent on sensitive personal data and its collection and processing. It is therefore proposed to categorise sensitive personal data and clearly define it. The present Act also does not regulate the risks of harms including material losses such as financial loss, loss of access to benefits or services, identity theft, loss of reputation, discrimination etc., arising out of processing of personal data. The Committee of Experts on Data Protection constituted by the Central Government in 2017 under the chairmanship of Justice B.N. Srikrishna to examine the issues relating to data protection in the country in its Report had observed that harm is a possible consequence of personal data processing and had recommended that it should be regulated under a data protection law. The Bill therefore proposes that explicit consent is mandatory for collection and processing of sensitive personal data. Further, it is proposed that in cases of withdrawal of consent by the data principal, the request must necessarily be processed and implemented within a stipulated time frame of thirty days. The Bill also seeks to restrict the retention of personal data.

In the DPDP Act, 2023, the provisions relating to Right to Data Portability and the Right to be Forgotten have not been included. Both these rights were part of the 2018 draft Bill and the Personal Data Protection Bill, 2019 introduced in Parliament and was recommended by the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019. The Srikrishna Committee (2018) had observed that a strong set of rights of data principals is an essential component of a data protection law and that these rights are based on the principles of autonomy, transparency and accountability to give individuals control over their data. The GDPR of the European Union also recognises these rights. The right to data portability allows data principals to obtain and transfer their data from data fiduciary for their own use in a structured, commonly used and machine-readable format, thus giving the data principals greater control over their data. It also facilitates migration of data from one data fiduciary to another.

The Right to be Forgotten refers to the right of individuals to limit the disclosure of their personal data on the internet and to have their personal data removed or erased in certain circumstances, such as withdrawal of consent or the purpose for which data was collected and processed has been served or the data is requested to be pulled down by the data principal for various reasons. Guaranteeing of this right is imperative in the present times when a person is often haunted by the data being retained in the digital world, irrespective of its veracity or contextual relevance, and has the power to cause damage to a person's right to life with dignity. The Srikrishna Committee (2018) observed that the Right to be Forgotten is an idea that attempts to instil the limitations of memory into an otherwise limitless digital sphere. However, the Committee has also highlighted that this right may need to be balanced with competing rights and interests and has laid down five-point criteria for determining its applicability. Several Court pronouncements have also recognised this right, particularly when it pertains to sensitive personal information and acquittals which if allowed to remain on digital platforms adversely affects the personal life of an individual, continued loss of respect, employment opportunities, matrimonial prospects and leads to discrimination and isolation in society. The present Bill therefore, proposes to incorporate the Right to be Forgotten subject to

the limitations based on the five-point criteria laid down in the Srikrishna Committee Report.

The Bill also proposes to omit the exemption given to certain class of data fiduciaries from giving the requisite notice before collection of personal data and obtaining consent for its processing. Though the present Act provides that the Data Protection Board of India will function as an independent body, the appointment of its Members for two years with eligibility for re-appointment is likely to lead to increased influence and control of the Executive. It is therefore, proposed that Members of the Board will be appointed for five years and will not be eligible for re-appointment, so that the independent functioning of the Board is not undermined.

The above-mentioned amendments will definitely give more teeth to our data protection framework and strengthen it sufficiently so that India can unleash the power of data and use it to its fullest potential in transforming our country and economy into one of the foremost powers in the world.

Hence this Bill.

SANDOSH KUMAR P.

ANNEXURE

EXTRACTS FROM THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

(22 OF 2023)

* * * * *

2. * * * * * Definitions.

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

* * * * *

(k) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary.

* * * * *

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;

* * * * *

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,— Grounds for processing personal data.

(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.

* * * * *

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,— Notice.

(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.

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.

* * * * *

(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.

* * * * *

Certain legitimate uses.

7. A Data Fiduciary may process personal data of a Data Principal for any of the 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.

* * * * *

General obligations of Data Fiduciary.

8. * * * * *

(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.

* * * * *

Right of grievance redressal.

13. * * * * *

(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.

* * * * *

Exemptions.

17. * * * * *

(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.

* * * * *

Salary, allowances payable to and term of office.

20. * * * * *

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

* * * * *

40. * * * * * Power to make rules.

(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:—

* * * * *

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

* * * * *

RAJYA SABHA

A

BILL

to amend the Digital Personal Data Protection Act, 2023.

(Shri Sandosh Kumar P., M.P.)

RS-P&PS–PMB(E)—059–10.02.2025.