AN ANALYSIS OF DIFFERENCES AND ADVANCEMENTS MADE BY THE DATA PROTECTION BILL 2023 COMPARE TO PREVIOUS RELEVANT DATA PROTECTION LAWS

Vidya M.N, Research Scholar, School of Law, Alliance University, Bengaluru

ABSTRACT:

The era of digitization has transformed our lives completely with the advancement of technology and cyberspace. The emergence of virtual world has brought numerous benefits, but it also distressed the personal life of an individual. When we use social media, online business, browsing, cloud storage we leave traces behind in the virtual world. As the data is easily reachable in the digital domain, the personal information can be used for malicious purposes by the hackers which may result in data breach, data mining and cyber security threats etc. Data privacy and data protection has become significant buzzwords nowadays. The main concern is awareness about data sharing, the security measures, process mechanism, accountability of ownership, transferability principles and so on.

To combat such cybercrime practices and to evade consequences of digital era, Indian government has come up with its own data protection law in the year 2023 known as Digital Personal Data Protection Act. The Act provides a wide-range safeguard for personal information in digital ecosystem.[1] The Act empower the individuals to understand how their data is being utilized and provide them with the ability to modify or delete their personal information. The Act is been considered as streamlined legal framework which reflects the contemporary standpoint concerning the principles of data protection balancing between obligations of corporate entities and rights of an individual.

Keywords: Data protection bill and Act, Sensitive personal data, Children personal data, Data Protection Board, Data sharing and data transfer.

[1] Ranjan Radha, Digital Personal Data Protection Act 2023: Safeguarding your Online Identity, ISBN: 978-93-5826-263-6, Pp. 108-118, (Ink of Knowledge Gujarat 2024).

INTRODUCTION:

The Digital Personal Data Protection Act, an historic piece of legislation is an attempt to bring a harmonized data privacy regime in India. The DPDP Act was passed by the Indian Parliament on August 2023.[2] The dedicated legal regime was enacted after more than half a decade of deliberations and it is the primary cross-sectoral regulation on personal data protection in India.[3] The Act aims to protect individual's identities in a digital technology world. It is a detailed framework which can handle the rising apprehensions about data breaches and unauthorized use of personal data. The new Act has provided more control to people who can expressly participate in process, storage, sharing and transfer of their data. In addition, the Act also covers cybersecurity measures which reinforces the digital platform. Compare to previous draft versions this new Act has come up with some significant alterations such as controllable rights of data principle, obligations to data fiduciary, mandatory consent, legitimate use and notice rule, control over processing and sharing of data, stringent provisions for cross-border data transfer, establishment of Data Protection Board replacing with Data protection Authority[4], specific exemptions for data fiduciaries and monetary penalties for data related crimes and so on.[5] The DPDP Act acknowledges at safeguarding privacy rights and promoting responsible data management practices. The Act aimed to strike a delicate balance between individual rights and an organization's legitimate data-processing needs. The Act gives equal merit for protection to all digital data, but the drawback is the act does not define any data category as sensitive personal data[6] or critical data. Unlike the SPDI Rules 2011, the DPDP Act does not categorizes personal data into personal data and sensitive personal data. The new Act recognizes all digitized personal data uniformly. The Act governs the collection and

---

[2] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), *Gazette of India,* August 11, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[3] Burman Anirudh, Understanding India's New Data Protection Law, Carnegie India 2023, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

[4] Data Protection Board established by the Central Government under Section 18 of the DPDP Act.

[5] Sengar, Sanket Singh, *From Pixels to Policies: Analysing the Provisions and Navigating the Complexities of the Digital Personal Data Protection Act, 2023* (August 22, 2023). Available at SSRN: https://ssrn.com/abstract=4547842 or http://dx.doi.org/10.2139/ssrn.4547842.

[6] In the absence of an express clarification within DPDP about what the term 'sensitive' connotes (or includes), the meaning of SPDI itself may be interpreted with reference to corresponding definitions under the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "**SPDI Rules**") and/or GDPR – or even by referring to past iterations of DPDP, such as the Personal Data Protection Bills of 2018 ("**PDP 18**") and 2019 ("**PDP 19**"), respectively, as well as the Data Protection Bill of 2021 ("**DP 21**," and together with PDP 18 and PDP 19, "**Prior DPDP Iterations**"). [Sense and Sensitivity: 'Sensitive' Information Under India's New Data Regime, 2023, https://www.snrlaw.in/sense-and-sensitivity-sensitive-information-under-indias-new-data-regime/]

processing of digital personal data, excluding any provisions related to non-personal data, which was covered in the PDP Bill, 2019.[7] As the nature of the Act strictly restricted to personal data in the digital realm, a significant issue arises from various clauses of the DPDP Act. In turn this situation gave rise to concerns about the possibility of unregulated and discretionary rule formulation.[8] The present chapter gives a comprehensive overview of the New Act. The chapter starts with discussing the importance of the Act, followed with the key concepts which are newly introduced under the Act. Subsequently, the chapter highlights on the major features of the legislation. Continuing with, it encompasses the nexus between the GDPR and previous bills and the new Act. In addition, the chapter discusses the lacunas of the Act, which needs to be viewed prudently.

INDIA'S DATA PROTECTION LAW – A JOURNEY SO FAR:

Before the DPDP Act, the dependency was only on IT Act and SPDI Rules for regulating data related issues.

The journey of adopting our own data protection law started with the advent of landmark judgement on right to privacy in the digital space by the Supreme Court in 2017. The Supreme court in K.S. Puttaswamy judgement[9] declared that the Right to Privacy is a part of fundamental right under the framework of Right to life (Article 21 of the Indian Constitution) and right to Information privacy is a part of this right.[10] The decision did not define any specific outlines of the right to information privacy and it also did not lay down specific mechanisms through which this right was to be protect.

Based on the recommendations of the Aadhaar judgement, on July 2018 the committee was formed under the chairmanship of Justice Srikrishna who submitted the report along with the draft of Personal Data Protection bill 2018. [11] The recommendations of the committee were

[7] Unlocking opportunities and navigating challenges: the impact of the Digital Personal Data Protection Act on M&A. EY Parthenon, March 2024. Available on https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/mergers-acquisitions/ey-unlocking-opportunities-and-navigating-challenges-the-impact-of-dpdp-act-on-m-a-march-2024.pdf.
[8] Sengar, *supra* note 2.
[9] K.S Puttaswamy and Anr V. Union of India and Ors., [(2017) 10 SCC 1]
[10] Burman Anirudh, Understanding India's New Data Protection Law, Carnegie India 2023, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.
[11] The Personal Data Protection Bill, 2018, accessed March 8, 2019, https://www.thehinducentre.com/resources/article24561526.ece/binary/Personal_Data_Protection_Bill,2018_0.

based on European Union's (EUs) General Data Protection Regulation (GDPR).

The Ministry of Electronics and Information Technology (MeitY) introduced the PDP Bill 2019 (The Personal Data Protection Bill, 2019)[12] in the Lok Sabha on December 2019. The scope of this draft version was wide and it recommended for cross-sectoral, economy-wide data protection law to be directed by data protection regulator (i.e., Data Protection Authority). The 2019 draft imposed a number of obligations on entities collecting personal data, such as provide notice and take consent from data principals. Data fiduciaries should require to delete data once the purpose was fulfilled and to provide consumers right to access, erase and port their data. corporate entities required to maintain security safeguards and transparency requirements, implement 'privacy by design' requirements, and create grievance redress systems. The bill introduced an entity known as 'consent managers' who were intermediaries for collecting and providing consent to businesses on half of individuals.[13] The PDP Bill categorized the personal data into 'sensitive and critical personal data'. And certain business entities were been categorized as 'significant data fiduciaries' by providing certain obligations for data audits and data impact assessments. Adding to this, the bill also levied data localization restrictions for cross-border data flow. The Data Protection Authority was authorized to impose penalties. The bill also proposed to criminalize activities related to deanonymization of individuals. The bill also had a provision for exemptions for certain entities from notice and consent requirements under certain circumstance such as lawful state functions, medical and health services during emergencies or epidemics, breakdown of public order, employment-related data processing, the prevention and detection of unlawful activity, whistleblowing, and credit recovery, among others. The bill also authorized the government to regulate nonpersonal data. In short, the 2019 bill was a comprehensive, cross-sectoral framework based on preventive requirements for data fiduciaries and data principals.[14]

The PDP Bill was referred to Joint Parliamentary Committee (JPC). On November 2020, the JPC suggested expanding the bill's scope with a focus on overall data protection that covers

[12] The parliament committee published a report December 2021. "Report of the Joint Committee on the Personal Data Protection Bill, 2019," 17th Lok Sabha Secretariat, December 16, 2021, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

[13] Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?," Carnegie India, March 9, 2020, https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217.

[14] Burman Anirudh, Understanding India's New Data Protection Law, Carnegie India 2023, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.

Personal and Non-personal Data. Further, on November 2021, JPC released its report with 81 amendments and 12 recommendations and with the expanded scope the JPC changed the name of the bill into Data Protection Bill.[15] On August 2022, the PDP Bill 2019 was withdrawn as its extensive scope was challenging and created a serious risk of overregulation and under-regulation.

Aiming to build a complete legal framework on the digital ecosystem, on November 2022, the MeitY released draft Digital Personal Data Protection Bill (DPDP Bill). [16] This draft bill was pretty different compared to the previous versions of bills.

Subsequently, on July 2023 the Union Cabinet approves the draft DPDP Bill 2023. Finally, on August 2023 the President assents to the Digital Personal Data Protection Act. Most awaited Act has finally passed by the Indian Government.

KEY TERMINOLOGIES UNDER THE DPDP ACT

The DPDP Act has come up with some new concepts suitable for information privacy which was a main focal point under the Act. Information privacy is the new nomenclature which emerged with the increase of presence of personal data in the digital form. The term 'Information Privacy' describes the person's ability to decide how and when their personal information is collected, shared and utilized.[17]

- *Consent* – Data fiduciaries/organizations should seek a consent, which is freely given, specific, informed and unambiguous indication of the Data Principal's wish.

- *Consent Manager* – A consent manager represents the Data Principal and takes

[15] 'Report of the Joint Committee on the Personal Data Protection Bill, 2019,' 17th Lok Sabha Secretariat, December 16, 2021, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

[16] The Digital Personal Data Protection Bill, 2022, Ministry of Electronics & Information Technology, Government of India, accessed August 9, 2023, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

[17] Kabra Shagun CA, Lad Jhyati, Advancement of Technology, lack of privacy: Pre-requisite of the Digital Personal Data Protection Act, 2023, 11(2) International Journal of Research and Analytical Reviews (IJRAR), 49-57 (2024).

action on their behalf when granting, managing, reviewing and revoking consent.[18]

- *Data* – represents information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human being or by automated means.[19]

- *Data Fiduciary* – Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.[20]

- *Data Principal* – any individual to whom the personal data relates, a child[21] or disabled person (including parent or guardian for consent purpose).[22]

- *Data Processor* – Any person who processes personal data on behalf of Data Fiduciary.[23]

- *Digital Personal Data* – represents personal data in digital form.[24]

- *Legitimate uses*[25] - Consent is not expressly needed for situation such as voluntary disclosure, disclosure with reasonable expectation, disclosure of data as a matter of performance of function under law, medical emergency, for the compliance with any judgement, disclosure to avoid threat to public health and data disclosure to ensure safety in case of any disaster.[26]

[18] 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.
[19] Sec. 2(h) of the DPDP Act
[20] Sec. 2(i) of the DPDP Act
[21] *Children's Data – for children below the age of 18, the consent from parent or guardians is required. Behavioural monitoring and targeted advertising are prohibited.*
[22] Sec. 2(j) of the DPDP Act, 2023
[23] Sec. 2(k) of DPDP Act, 2023
[24] Sec. 2(n) of DPDP Act
[25] Legitimate uses are defined as: (a) a situation where an individual has voluntarily provided personal data for a specified purpose; (b) the provisioning of any subsidy, benefit, service, license, certificate, or permit by any agency or department of the Indian state, if the individual has previously consented to receiving any other such service from the state (this is a potential issue since it enables different government agencies providing these services to access personal data stored with other agencies of the government);[15] (c) sovereignty or security; (d) fulfilling a legal obligation to disclose information to the state; (e) compliance with judgments, decrees, or orders; (f) medical emergency or threat to life or epidemics or threat to public health; and (g) disaster or breakdown of public order.
[26] The Digital Personal Data Protection Act, 2023 – Advent of Privacy era in India, EY 2023.

- *Notice* – Notice should be clear, itemized and in simple language.

- *Processing outside India* – Government to notify countries to which transfer is not permissible unlike the whitelisting approach under the EU GDPR.

- *Personal Data* - any data about an individual who is identifiable by or in relation to such data.[27]

- *Processing* – 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, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.[28]

- *Signified Data Fiduciary (SDF)* – any Data Fiduciary or class of Data Fiduciaries notified to act as a SDF by the Central Government.[29]

VARIOUS CANONS OF THE DPDP ACT

The DPDP Act has come up with a new look by providing suitable provisions for privacy era. Compared to the 2019 PDP Bill, the new Act is quite modest. The structure of the regulation is simpler. The Act has precisely included certain features which necessitated to combat the cyber space and information privacy related issues. The Act provides for detailed procedure for data collection, data processing, data storage and transfer and Act also prescribes the rights and duties of Data principal and Data fiduciary and so on.[30] Let us look into the major norms of the DPDP Act.

- ***Applicability of the Act***

  The DPDP Act applies within and outside the Indian territory for processing of digital and digitized personal data (for lawful purpose and with individual consent), where the personal

[27] Sec. 2(t) of the DPDP Act, 2023
[28] Sec. 2(x) of the DPDP Act
[29] Sec. 2(z) of the DPDP Act
[30] The Digital Personal Data Protectino Act, 2023, PWC, https://www.pwc.in/assets/pdfs/consulting/risk-consulting/the-digital-personal-data-protection-act-india-2023.pdf

data is collected in a digital form and non-digital form and digitized subsequently and applies to any activity related to offering of goods or services to data principals within the territory of India.[31]

On the other hand, the Act does not apply to personal data processed by an individual for any personal or domestic purpose and personal data that is made or caused to be made publicly available by the data principal to whom such personal data relates. In addition, the Act will not be applicable for person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.[32]

The DPDP Act provide certain exemptions for the applicability of law. When a personal data is processed for the purpose of enforcing legal right, prevention, detection, investigation or prosecution (of any offence) or contravention, scheme of compromise, arrangement, merger, amalgamation etc.,[33] such circumstances can have exemption. And, if any contract is entered into with any person outside the territory of India by any person based in India, applicability of law will be exempted. Adding to this, under certain situations the Data fiduciaries (including start-ups with the notification of Central Government), and Central and State Governments will be exempted from the Act.[34]

- ***Consent and Consent withdrawal:***

When the Data is collected from the Data Principal the consent and consent withdrawals[35] principles are essential. The Consent taken by the Data Principal should be free, specific, informed, unconditional and unambiguous with a clear affirmative action and signify an agreement to the processing of personal data [the consent must be freely given and should be explicit, specific, informed, unconditional, clear-cut and revocable].[36] The data principal has a right to withdraw the consent[37] at any time. Upon such withdrawal, the data fiduciary shall cease processing the personal data of such individual unless it is required.

[31] Sec. 3(a) and (b) of the DPDP Act, 2023
[32] Sec. 3(c) of the DPDP Act, 2023
[33] Kabra Shagun, *supra* note 414.
[34] Sec. 17 of the DPDP Act
[35] Chapter II, Section 6 of the DPDP Act deals with Consent and Consent withdrawal.
[36] According to Sec. 6(1) of the Act, Consent means an indication by the data principal signifying an agreement for their data to be processed for a specified purpose and be limited to such personal data as is necessary for such specified purpose.
[37] As obligated under Section 6(7) of the DPDP Act, 2023.

- ***Childrens' Data:***

  The DPDP Act imposes additional obligations for data processing related to child[38] (child – below the age of 18 years [Section 2(f)]. Such as:

  - A requirement to obtain verifiable parental consent or that of a lawful guardian before processing children's data.[39] (the age of such individual must be verified)
  - Restrictions on processing that are likely to cause detriment to a child.[40]
  - A prohibition on tracking, behavioural monitoring and targeted advertising to children.[41]
  - The Central Government may lower the age of criteria from 18 years, 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.[42]

  Based on the abovementioned conditions the data fiduciary can claim for exemptions.

- ***Obligations of Data fiduciary:***

  The DPDP Act provides certain obligations for Data Fiduciaries. Stating to the Data Collection, the Notice[43] is required and in case of minor or disabled person before collecting data the consent has to be verified by the parent or guardian[44]. The notice should contain details about personal data which is to be collected, the purpose of processing, rights of the data principal and the way in which the rights can be exercised.

  Referring to Data processing, the Act provides for certain grounds for processing of personal data.[45] Such as the data should be obtained only for certain legitimate use and for

[38] Sec. 9 of the DPDP Act
[39] Sec. 9(1) of DPDP Act
[40] Sec. 9(2) of DPDP Act
[41] Sec. 9(3) of DPDP Act
[42] Sec. 9(5) of DPDP Act
[43] Chapter II, Section 5 of the DPDP Act deals with Notice.
[44] Chapter II, Section 9 of the DPDP Act prescribes provision for Guardian consent and processing children's personal data.
[45] Chapter II, Section 4 & 7 of the DPDP Act deals with Grounds of processing personal data and Certain legitimate uses.

lawful purpose. The data can be processed to offer any benefit, subsidy, certificate, permit or license to data principal if previously consent is taken.[46]

Mentioning to the Data storage, the data fiduciary shall protect personal data in its possession by taking reasonable security safeguards to prevent personal data breach.[47] In such event of data breach, the data fiduciary shall give a notification of intimation to the board and affected data principal. Further, the Act provides for data retention policies.[48] Accordingly, the data fiduciary shall, unless retention is necessary for compliance with any law, erase personal data upon the withdrawal of consent by the data principal or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier.

For obligation of Transparency and accountability, the Data fiduciary is accountable for data processor[49]. The Data Protection Officer and Consent Managers are been appointed to fulfill such obligations. The data principal may give, manage, review or withdraw consent through a consent manager. He will be accountable for data principal. In case of need, the data fiduciary can act as a significant data fiduciary (SDF) to assess the factors such as volume and sensitivity of personal data processed, risk to the right of data principal, the potential impact on the integrity of India, security and public order of the State[50]. Such SDF may appoint Data Protection Officer, an Independent Data Auditor and may undertake compliance measures including Data Protection Impact Assessment (DPIA). [51]

- ***Cross-border Data transfer and Data Localisation:***

In relation to cross-border data transfers, while processing of personal data outside India, the Government by notification, can restrict the transfer of personal data by a data fiduciary[52]. Based on the exemption mentioned under the Act the personal data can be

[46] Sec. 7 of the DPDP Act, 2023
[47] Chapter II, Section 8 of the DPDP Act provides for Security safeguards and data processor obligations.
[48] Chapter II, Section 8 of the DPDP Act provides for Data retention.
[49] Chapter II, Section 8 – provides for Data processor engagement [Data fiduciary may engage, appoint, use or otherwise involve a data processor to process personal data on its behalf only under a valid contract]
[50] Chapter II, Section 9 – Additional obligations of significant data fiduciary (SDF).
[51] Sec. 10(2) of the DPDP Act
[52] Chapter IV, Section 16 provides for Processing personal data outside India.

processed outside India, in pursuant to any contract entered with such person outside the territory of India.

With regard to data localization the new regulation does not prescribe any specific requirements. It recognizes sector-specific laws which may have requirements to localize different categories of data, which may include personal data.[53] 2019 bill restricted certain data flows, while the 2023 act only states that the government may restrict data flow/transfer to specific countries through notification.

- ***Rights and duties of Data Principal:***

For the sake of data processing, storage and transfer the Act provides certain rights[54] and duties to Data principal[55] such as

(1) Right to access information – Data principal have the right to seek information on how their data is processed, available in clear and understandable way.[56] Every individual should have a knowledge about their whereabouts. To secure his interests not only morally, but legally also he should have a right to acquire basic knowledge about their personal information. With this view, the DPDP Act provides to every individual (data principal), a right to request a clarification about the details of data processing and data sharing.

(2) Right to correction, completion, updating and erasure – Individuals have the right to request for correction of inaccurate and incomplete data, updation of new information and erase of data that is no longer required for processing (exception is retention principle as a legal obligation).[57]

[53] Are there data localization / data residency or other types of laws that may require the retention and storage of personal data in the local jurisdiction? December 2023, Baker McKenzie Resource Hub, https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/india/topics/data-localizationresidency#:~:text=While%20the%20DPDP%20does%20not,which%20may%20include%20personal%20data.

[54] Sec. 12(2) and Sec. 14 of DPDP Act, 2023

[55] Chapter III of the DPDP Act deals with Rights and Duties of Data principal.

[56] Sec. 11 of the DPDP Act, 2023

[57] Sec. 12 of the DPDP Act, 2023

(3) Right of grievance redressal – Individuals have the right to readily available means of registering a grievance with a Data Fiduciary.[58] Data fiduciary is having a obligation to provide a grievance redressal mechanism to data principal. An aggrieved person has a right to approach data protection officer (appointed by the data fiduciary). In case of dis-satisfaction with the response of DPO, the data principal will have a right to register a complaint before Data protection board.

(4) Right to nominate – Individuals can nominate any other individual to exercise these rights in the event of death or incapacity.[59] The Act provides a right to data principal to nominate any person as his/her nominee, in case of death or incapacity to exercise the rights available to him.

Subsequently, the data principal shall have certain duties for the processing of data such as he should not suppress any material information while providing personal data, should not register a false or frivolous grievance or complaint, should furnish only such information which is verifiable authentic, and must not impersonate another person while providing personal data for a specific purpose.[60]

- ***Exemptions under the Act***

1. The Central Government is exempted from the processing of personal data used for

   a. Sovereignty and integrity of India, security of the State, friendly relations with foreign states, maintenance of public order.

   b. And for research, archiving or statistical purposes.

2. The DPDP Act exempts Data Fiduciary from certain obligations[61] (except for being responsible for its data processor and taking reasonable security safeguards) under specified circumstances including:

[58] Sec. 13 of DPDP Act, 2023 [With reference to the Right to Grievance redressal, the timeline to respond to grievances raised by the Data principals shall be notified by the Central Government].
[59] Sec. 14 of the DPDP Act, 2023
[60] Sec. 15 of DPDP Act, 2023
[61] Sec. 17(1) of DPDP Act 2023

a. Processing for enforcing any legal right or claim.

b. Processing for performance of any judicial or quasi-judicial functions by any Indian court/tribunal or other body.

c. Processing in the interest of prevention, detention, investigation or prosecution of any offence of any law.

d. Processing of Data Principals outside the territory of India pursuant to any contract entered into with any person outside the territory of India by the person based in India.

e. Processing necessary for a merger / amalgamation or similar arrangement as approved by a court or other authority competent.

- ***The Data Protection Board*** [62]

The DPB is an independent body established by the Central Government. The DPB is not a regulatory entity. Compare to Data Protection Authority, the DPB does not have any power to frame regulations. The Board is consisting of chairperson and other members. The Board has been entrusted with the task of enforcement, including determining non-compliances, imposing penalties, issuing direction and medication to ensure compliance with law.[63] The DPB has the power to receive complaints from the data principal and may proceed with the inquiry after determining sufficient grounds. The DPB may also issue interim orders. The DPB is enshrined with the powers of a civil court and appeals against its decisions before Telecom Disputes Settlement and Appellate Tribunal is allowed.[64]

- ***Penalties***

The Act also provides for Data Protection Board for penalty, grievance redressal, review and appeal and dispute resolution purposes. Schedule I of the Act provides for the

[62] Chapter V of the DPDP Act
[63] Sec. 27 & 28 of the DPDP Act, 2023 [the DPB performs numerous functions, such as immediate remedial or mitigation steps in the event of data breach, imposing penalties, determining adequate grounds to proceed with an inquiry, issuing interim orders and issuing a warning or cost in the case of frivolous complaints]
[64] Sec. 29 of DPDP Act, 2023 [any aggrieved party with Board's direction or order, can file an appeal before the Appellate Tribunal within 60 days from the data of receipt of direction. The appeal must be decided within 6 months from the data of appeal presented].

imposition of monetary penalty for noncompliance incidents, based on the kind of violations. The Data fiduciary will be penalized with huge amount in case of breach or non-compliance with such duty assigned to him.[65] The provision of penalty is also applicable for Data principal in case of breach or non-compliance of observance of his duties.[66]

- ***Data Protection Principles:***

Although the DPDP Act does not expressly refer to data protection principles, the Citizen's Data Security and Privacy Report submitted to the Lok Sabha on 1st August 2023, that outlines the Act's legislative history and key considerations, explain their explicit connection to the requirements of the law and their similarity to internationally recognized standards.[67] For instance, the law includes provisions that govern:

- Legality and Transparency – Every person that processes personal data must do so in accordance with the law, have a lawful purpose and meet transparency requirements when collecting consent from the data principal.[68]

- Purpose Limitation – Data fiduciaries must specify a purpose of processing and describe the personal data involved in the processing.[69] When relying on consent, the processing must only be necessary to achieve the stated purpose.[70]

- Accuracy and Completion – Section 8(3) requires data fiduciaries to ensure the personal data they process is accurate, complete and consistent.

[65] Sec. 33(1) & (2), Sec. 42(1) and Schedule of the DPDP Act 2023 - The major penalties are the DPB has the power to issue penalties up to INR 250 crore, Data fiduciaries are liable to pay a penalty up to INR 250 crore for breach in observing the obligation of a data fiduciary to take reasonable security safeguards to prevent personal data breach. Other penalties are, if the data fiduciary breaches in observing the obligation to give the board or affected data principal notice of a personal data breach, may lead to the penalty of INR 200 crore. In case of non-compliance of observance of the additional obligations of significant data fiduciary the penalty is INR 150 crore. In case of breach in observance of additional obligation in relation to children the penalty is INR 200 crore. And in case of non-compliance of any other provision of the Act the penalty is INR 50 crore.
[66] The penalty for Data principal in case of non-compliance of any such duty assigned to him is INR 10,000.
[67] Decrypting India's New Data Protection Law: Key Insights and Lessons Learned, Bird&Bird, 2023, https://www.twobirds.com/en/insights/2023/global/decrypting-indias-new-data-protection-law-key-insights-and-lessons-learned.
[68] Referring to Sec. 4 & 6 of the DPDP Act 2023
[69] Sec. 5(1) of the DPDP Act
[70] Sec. 6(1) of the DPDP Act

- Security and Integrity – Data fiduciaries must implement appropriate technical and organizational measures and take reasonable security safeguards to prevent unauthorized disclosures.[71]

- Storage Limitation – the Act also requires data fiduciaries (except for state bodies) to cease retention and delete personal data as soon as the purpose for which the data was collected has been achieved, and if the retention is no longer necessary pursuant to any legal obligation.[72] These conditions may be limited by other factors, such as where the data principal approaches the data fiduciary for the performance of a specified purpose or to exercise any of her rights.[73]

- ***Amendments to prevailing laws***

  The existing Information Technology Act 2000 and Right to Information Act 2005 are amended with the passing of DPDP Act. Section 43(A) referring to the compensation for failure to protect data of IT Act 2000 is omitted. And Section 8(1)(j) of the RTI Act 2005 is amended to exempt the personal information which allows disclosure for public interest.

COMPARISON BETWEEN PREVIOUS PERSONAL DATA PROTECTION BILLS AND CURRENT DIGITAL PERSONAL DATA PROTECTION ACT 2023[74]

The DPDP Act is a notable move in the approach toward data protection compare to previous draft bills.

- ***Scope and Applicability:***

  The Personal Data Protection Bill 2018 – the law applies to processing of personal data within and outside India if it is for business carried on, offering of goods and services or

[71] Sec. 8(4-5) of the DPDP Act 2023
[72] Sec. 8(7) of the DPDP Act 2023
[73] Sec. 8(8) of the DPDP Act 2023
[74] Sources: The Draft Personal Data Protection Bill, 2018; The Personal Data Protection Bill, 2019 and the Digital Data Protection Bill, 2023 as introduced in Lok Sabha ; Report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019; PRS, The Digital Personal Data Protection Bill, 2023, Ministry: Electronics and Information Technology, PRS Legislative Research, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

profiling individuals in India.

The Personal Data Protection Bill 2019 – the bill expands the scope to cover certain anonymized personal data compare to 2018 bill.

Joint Parliamentary Committee recommendation – compare to 2018 bill the JPC recommended to expand the processing of non-personal data and anonymized personal data.

The Digital Personal Data Protection Bill 2023 – the bill does not include offline personal data and non-automated processing of data.

- ***Reporting of data breaches:***

The Personal Data Protection Bill 2018 – Under this bill, the Data Fiduciary has a duty to notify to the Data Protection Authority about the breach of data which is likely to cause harm and the Authority will be deciding whether this has been notified to the data principals or not.

The Personal Data Protection Bill 2019 – with regard to the data breach reporting the 2019 bill is having same rule as 2018 bill.

Joint Parliamentary Committee recommendation – compare to 2018 bill the JPC recommended that all breaches, regardless of the potential harm, should be reported to the Data Protection Authority within 72 hours of the breach.

The Digital Personal Data Protection Bill 2023 – the 2023 bill added an effective feature relevant to data breach. Accordingly, every personal data breach must be reported to the Data protection Board of India and should be notified to each affected data principal in a prescribed manner.

- ***Provision of Exemptions for the security of the State, public order and prevention of offences etc.:***

The Personal Data Protection Bill 2018 – according to the bill the data processing must be authorized pursuant to the law and in accordance with the procedure established by law and

it must be necessary and proportionate.

The Personal Data Protection Bill 2019 – 2019 bill has restricted the processing of data for agencies. Accordingly, the Central Government by making an order may exempt agencies to process the data only if it is necessary or expedient and subject to certain procedure, safeguards and oversight.

Joint Parliamentary Committee recommendation – the JPC recommendation added another restriction to the Central Government order. It added the order must specify a procedure which is fair, just and reasonable.

The Digital Personal Data Protection Bill 2023 – the 2023 bill changed the JPC recommendation fully. the provision describes that the Central Government may exempt by notification, which does not require any procedure or safeguards to be specified.

- ***Right to Data Portability and Right to be forgotten:***

The Personal Data Protection Bill 2018 – Under the 2018 bill the Data Principal has right to data portability (i.e., to obtain data in interoperable format) and right to be forgotten (i.e., to restrict disclosure of personal data over internet).

The Personal Data Protection Bill 2019 – the bill provided for both the rights same as 2018 bill.

Joint Parliamentary Committee recommendation – The JPC also recommended for both the rights for Data Principal.

The Digital Personal Data Protection Bill 2023 – Compare to previous bills, the 2023 bill did not provide for any such right to Data Principal.

- ***Destruction from processing of personal data:***

The Personal Data Protection Bill 2018 – under this bill the harm relate to processing of data includes monetary loss, identity theft, loss of reputation and unreasonable surveillance. It is the duty of Data Fiduciaries to take measures to minimize and mitigate risks of harm.

On the other-hand the Data principal has a right to seek compensation for such harm which resulted through processing of personal data.

The Personal Data Protection Bill 2019 – relevant to processing of data and resulting into any harm, the bill followed the same provision based on 2018 bill.

Joint Parliamentary Committee recommendation – JPC recommended that the Central Government should have powers to prescribe additional harms if required along with the previous remedies available for harm while processing of data.

The Digital Personal Data Protection Bill 2023 – the bill does not provide for any such provision regard to harm from processing of personal data.

- ***Who is referred as a regulator:***

The Personal Data Protection Bill 2018 – the bill provided for establishing the Data Protection Authority of India to regulate the sector and for Appellate Tribunal.

The Personal Data Protection Bill 2019 – the bill also provided for the DPA and Appellate Tribunal.

Joint Parliamentary Committee recommendation –The JPC also recommended for the establishment of DPA and Appellate Tribunal.

The Digital Personal Data Protection Bill 2023 – the bill provided for Data Protection Board (DPB) of India whose primary function is to adjudicate non-compliance. And Telecom Disputes Settlement and Appellate Tribunal (TDSAT) has been designed as the Appellate Tribunal.

- ***Personal data transfer outside India:***

The Personal Data Protection Bill 2018 – under this bill it is the duty of every fiduciary to store at least one serving copy of personal data in India. And with the consent from data principal the data may be transferred outside India for certain permitted countries under the contracts approved by the Data protection Authority. With regard to critical data, it can be processed only within India.

The Personal Data Protection Bill 2019 – the bill provided a provision through which a copy of sensitive data should remain in India. And with the explicit consent the sensitive personal data can be transferred (no such restriction for any other personal data). Relevant to critical data the rule is same as 2018 bill.

Joint Parliamentary Committee recommendation – The JPC recommended that the sensitive personal data will not be shared with foreign agencies or government, without the prior approval of the Central Government.

The Digital Personal Data Protection Bill 2023 – the bill removed sensitive and critical personal data classification. And the transfer of personal data can be restricted to certain countries through notification by the Central Government.

DIFFERENCE BETWEEN EU GDPR AND INDIA'S DPDP ACT

The EU GDPR is one of the most remarkable regulation, which acts as encyclopedia for data protection regimes at the international arena. After the emergence of GDPR in 2018, majority of the world countries came up with their own Data protection laws with a holistic approach towards the fast-growing technology era. Factually, to be specific the new DPDP Act also has emerged as a follower of GDPR. During the journey of drafting India's data protection law, the GDPR has acted as a key foundation. Certain provisions are been adopted and incorporated into current India's Data protection law. Hence, it is a need to the researcher to analyze the nexus between European Union's General Data Protection Regulation 2018 and Digital Personal Data Protection Act 2023 of India. Major differences between GDPR and DPDP are as follows:

- *Application of law*: The GDPR applies to processing of Personal Data wholly or partly by automated means and to Personal Data which form or will form a part of a filing system. The DPDP Act will apply to digitized personal data and non-digitized personal data which is subsequently digitized.

- *Penalty* – Penalties under GDPR extend to 20 million euros or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. On the other hand, penalties under the DPDP Act extend up to INR 250 crore.

- *Consent to children's data* – Minor under the age of 16 need parental consent. Members states of Europe can lower this age to 13 for their regions. Under DPDP, children under the age of 18 need consent from parents/guardians.

- *Data Breach Notification* – under GDPR, breaches should be notified to the Supervisory Authority within 72 hours and possibly to the affected Data Subjects. Under DPDP Act, it does not specify a timeframe for Personal Data Breach notification.[75]

- *Right to Nominate* - GDPR does not include right to nominate however provides for the right to portability. Organizations have 30 days to respond to a Data Subject request. The DPDP Act comprises of an additional right to nominate while omits the right to portability and timeline to respond to the Data Principal requests has not been specified.

- *Transfer of Data* – GDPR lays down specific mechanisms for transferring data to third country such as standard contractual clauses and binding corporate rules. On the other hand, the DPDP Act has not identified any transfer mechanisms for transferring Personal Data.

- *Data Protection Officer* – Under GDPR, both Controllers and Processors are under the obligation to appoint a DPO in specific circumstances. Under DPDP Act, only the Significance Data Fiduciary (SDF) shall have to appoint DPO as a point of contact for the Data Protection Board.

- *Recording of processing activities* – Under GDPR, Data Controller and Data Processor are required to maintain the records of processing activities (ROPA). But under DPDP Act, it does not include any obligation for Data Fiduciaries to main records of processing activities.

[75] Advent of Privacy Era in India – The Digital Personal Data Protection Act, 2023, EY, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/cybersecurity/2023/08/ey-dpdp-act-placemat.pdf?download#:~:text=Personal%20data%20made%20publicly%20available.&text=An%20individual%20to%20whom%20the,guardian%20acting%20on%20their%20behalf.&text=Non%2Dreporting%20of%20breaches%20%2D%20The,safeguards%20falls%20on%20data%20fiduciaries.

- *Data Protection Impact Assessment* – under GDPR the Data Protection Impact Assessment (DPIA) is to be conducted by Data Controllers for all the high-risk processing activities. Under DPDP, Significant Data Fiduciaries are obligated to conduct periodic Data Protection Impact Assessment.

LACUNAS OF DPDP ACT

- ***Discretionary authority upon the Central Government*:**

  The DPDP Act provides discretionary authority upon the Central Government to exempts specific data fiduciaries (SDF) for handling of data. Furthermore, the Act allows the Central Government (within a span of 5 years from the Commencement of the Act) to exempt certain data fiduciaries or groups of them from any provisions of the DPDP Act for a specific period.

  The Act also includes provisions that allow the State to be exempt from certain regulations, potentially causing negative implications for privacy.

- ***Exemptions to data fiduciaries*:**

  The DPDP offers exemptions to data fiduciaries from certain obligations, excluding the requirement to implement reasonable security measures for personal data protection. One such instance is when processing personal data of individuals not located within the territory of India, as part of a contract formed with individuals outside India. This particular provision appears to alleviate the compliance burden for entities involved in business process outsourcing activities.

- ***Handling of personal data*:**

  The Act fails to address and control the potential damage caused by the handling of personal data. The Srikrishna Committee (2018) recognized that the harm can be a outcome of personal data processing, such as financial loss, denial of benefits, identity theft, damage to reputation, discrimination and excessive surveillance and profiling. In response, the committee recommended to regulate such harm through data protection law.

- ***Violation of Right to Privacy*:**

  Through 2017's landmark judgement, SC ruled that any violation of the right to privacy must be balanced with a legitimate need for such intrusion. Instances where the State is granted exceptions could result in excessive gathering, manipulation and storage of data beyond what is essential. Such actions might not be in proper proportion and could potentially infringe upon the core right to privacy. The legislation grants the central government the authority to waive certain provisions for government agencies, citing reasons such as State security and upholding public order. Specific scenarios, like data processing for preventing, investigating and prosecuting offences, would not be subject to the usual rights of data subjects and responsibilities of data handlers, barring data security. The legislation does not mandate government agencies to erase personal data after its processing purpose is fulfilled. By employing these exceptions, particularly in the name of national security, a government entity could gather citizens' information to construct a comprehensive surveillance profile. This might involve utilizing data retained by diverse government bodies. This situation prompts scrutiny regarding whether these exceptions align with the principle of proportionality.[76]

- ***Absence of the provision for 'Right to Data Portability' and the 'Right to be Forgotten'***

  The right to data portability empowers individuals to acquire and transfer their information from a data controller in a format that is organized, commonly used, and machine-readable. This right offers individual enhanced authority over their data and might simplify the process of moving data from one data controller to another. An apprehension in this context is that it could potentially disclose proprietary business information of the data controller. The Srikrishna Committee in 2018 suggested that if it is feasible to provide the data without exposing such confidential information, the right should be ensured. The Joint Parliamentary Committee noted that the protection of trade secrets shouldn't be a valid reason to deny data portability; the denial should only occur based on technical feasibility.

  The right to be forgotten pertains to individuals' entitlement to restrict the exposure of their personal information on the internet. The Srikrishna Committee in 2018 noted that the right

[76] Sengar, Sanket Singh, *From Pixels to Policies: Analysing the Provisions and Navigating the Complexities of the Digital Personal Data Protection Act, 2023* (August 22, 2023). Available at SSRN: https://ssrn.com/abstract=4547842 or http://dx.doi.org/10.2139/ssrn.4547842.

to be forgotten is a concept aiming to introduce the limitations of human memory into an otherwise boundless digital realm. However, the Committee also underscored that this right must be carefully weighed against conflicting rights and interests. The exercise of this right could potentially impinge on another person's right to freely express themselves and access information. Decisions regarding its applicability could be influenced by factors like the sensitivity of the data to be suppressed, the pertinence of that data to the public, and the role the individual holds within the public sphere.

The legislation does not include provisions for the rights of data portability and the right to be forgotten. These rights were, however, included in both the 2018 bill and 2019 bill that were presented in Parliament. The Joint Parliamentary Committee, which evaluated the 2019 bill, advised that these rights should be preserved. There rights are also acknowledged in the GDPR framework. The Srikrishna Committee in 2018 emphasized that a robust set of data subject rights is a fundamental aspect of a data protection law. these rights, grounded in principles of self-determination, transparency and responsibility, empower individuals to manage their data.

- ***Lessening the rights and obligations and compliance***

Detailed prescriptions regarding the contents of notices and privacy by design requirements have been discarded and it is now up to business entities to translate these requirements.

CONCLUSION

The introduction of the DPDP Act marks a pivotal milestone in the realm of safeguarding personal data within India. This development was long-awaited, considering the considerable number of internet users in the country, the voluminous data generated by them and India's substantial involvement in cross-border trades and investments. While the existing laws provide certain protections for data principles and lay out obligations for data processors, incident reporting and other aspects, the current regulatory frameworks lack comprehensiveness and solidity.

The DPDP Act represents a substantial transformation by overhauling the existing framework and replacing the current laws. It is a substantial stride toward enhancing the protection of individual privacy in India. By establishing a more transparent and accountable system for the

processing of personal data, the DPDP empowers individuals with greater control over their own personal data. Importantly, this Act offers a significant advancement in guarding individuals against the inappropriate use of their personal data and amplifies their ability to assert their individual rights pertaining to their personal data. This legislative initiative is poised to play a key role in shaping the data protection landscape and ensuring the privacy and security of individuals' information in India.

Nevertheless, the DPDP is not immune to criticism. Some critics may contend that it carries excessive restrictions that could potentially stifle innovation within the industry. Conversely, others might argue that the DPDP falls short in adequately safeguarding individual privacy due to the considerable authority granted to the Central Government in relation to personal data processing.

The forthcoming steps will shed light on how the Central Government shapes regulations through delegated legislation to address aspects of the DPDP that remain unspecified. The repeated use of the phrase 'as may be prescribed' throughout the DPDP underscore the importance of the Central Government establishing a systematic approach for formulating and releasing these diverse regulations. It would be beneficial for the Central Government to engage in consistent consultations with stakeholders spanning various sectors to ensure comprehensive insights are gathered. MeitY's track record in conducting such consultations, as demonstrated in the recent amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 for online gaming in April 2023, showcases the potential for achieving industry alignment and balanced regulations.

These regulations should take into account the practicalities of the industry, thus fostering a robust data protection framework that ultimately serves the interests of the entire technology sector in India.

Finally, it is imperative to establish a transition period that affords businesses ample time to organize essential procedures and conform to the stipulations of the DPDP. Given the introduction of more stringent obligations, data fiduciaries could face a substantial amount of work to ensure compliance. Implementing the DPDP without an appropriate transition period could lead to widespread non-compliance, potentially causing significant disruptions.

Providing a substantial transition window will facilitate a seamless adjustment process for businesses, allowing them to align their operation with the guidelines set forth in the DPDP. This approach promotes a smoother transition and enhances the likelihood of comprehensive adherence to the new regulations.