Reg:Office: No 37, "Ujvala", 20th Main, BSK First Stage
Bengaluru: 560050
Ph: +91 8310314516: E Mail: fdppi@fdppi.in: web: www.fdppi.in
GSTN: 29AADCF4963H1ZC

FDPPI
Think Data, Think FDPPI
Section 8 Company (Not for Profit), Limited by Guarantees

Understanding Digital Personal Data Protection Act, (DPDPA) 2023 of India

Mr. M.G.Kodandaram, IRS.
Assistant Director (Retd)
ADVOCATE and CONSULTANT

Introduction

The eagerly awaited Digital Personal Data Protection Bill (DPDP) of 2023 was introduced in the Lok Sabha on August 3, 2023. Following its subsequent endorsement by both houses of the parliament, the Digital Personal Data Protection Act of 2023 (No. 22 of 2023) (DPDPA) received official presidential approval on August 11, 2023. The primary goal of the DPDP Act, succinctly referred to as the Act, is to establish a comprehensive regulatory framework for the management of digital personal data. This framework is designed to uphold individuals' rights to safeguard their personal information while also recognizing the legitimate needs and purposes for processing such data.

The Act places a strong emphasis on safeguarding privacy, while also acknowledging the critical role of stimulating innovation and driving economic growth. It provides clear guidelines for businesses to handle personal data responsibly, promoting ethical and data-driven practices that align with individuals' privacy rights. The key components of this pivotal Act are briefly explored in the subsequent sections.

India currently lacks an independent statute solely dedicated to safeguarding personal data. The responsibility for overseeing the use of personal information falls within the jurisdiction of the Information Technology (IT) Act of 2000. Recognizing this gap, in 2017, the central government established a commission of experts on data protection, led by Justice B. N. Srikrishna. This panel was entrusted with the crucial task of addressing the complex landscape of data protection within the country. During this period, the Hon' Supreme Court of India ruled in the landmark Puttaswamy case that the right to privacy is an intrinsic component of the broader right to life as outlined in Article 21 of the Constitution of India. This decision underscored the fundamental nature of privacy rights in the Indian legal context.

In July 2018, the commission submitted its comprehensive report, laying the groundwork for future privacy data protection legislation. Building upon the recommendations set forth in this report, the Personal Data Protection Bill (PDPB)of 2019 was introduced in the Lok Sabha in December of that year. Subsequently, the bill underwent scrutiny by a Joint Parliamentary Committee, culminating in the presentation of its findings in December 2021. However, the bill's progress was halted in August 2022 when it was withdrawn from parliamentary proceedings. This setback led to the release of a Draft Bill for public feedback in November 2022. After considering the inputs from various stakeholders, the Digital Personal Data Protection Bill of 2023 was eventually presented in Parliament in August of this year. This significant piece of legislation has now been enacted as the binding law of the nation, solidifying India's stance on safeguarding digital personal data in a manner that respects individual privacy rights and aligns with contemporary data-driven imperatives.

Applicability of the Act

The scope of the Digital Personal Data Protection Act encompasses the handling of '*digital personal information*' within India's borders. This law applies to collected personal data, either originally in digital format or converted to digital form after being initially gathered in a non-digital format. Furthermore, the law is also relevant to the processing of digital personal data outside of India's territory, provided such

processing is linked to activities involving the provision of goods or services to individuals within India. [section 3]. Provisions of this legislation will become effective from a date notified by the Central Government and separate dates can be designated for distinct provisions also. In relation to this enactment:

(a) The term "data" pertains to a depiction of information, encompassing realities, notions, viewpoints, or directives, conveyed in a manner appropriate for human comprehension, transmission, construal, or automated handling. [section 2(h)].

(b) The adjective "Automated" refers to any digital process with the capacity to function autonomously in response to designated instructions or other stimuli with the intent of processing data. [section 2(b)].

(c) The expression "Personal data" encompasses any information linked to an identifiable individual or connected with such data. [as specified in section 2(t)].

(d) The term "Digital personal data" signifies personal data exhibited in a digital configuration. [section 2(n)].

The Act recognizes the "Data Principal" (herein after 'principal, for brevity) as the individual to whom the personal data pertains. If this individual is a child, it encompasses the child's parents or lawful guardian. In the case of a person with a disability, their lawful guardian is included when acting on their behalf (section 2(j)). A "child" denotes a person under eighteen years old (section 2(f)).

However, this law does not apply to the following situations:

a) Personal data managed by an individual for personal or domestic intentions.

b) Personal data that has been intentionally disclosed to the public by the Data Principal to whom the data pertains or by any other individual compelled by prevailing Indian laws to make such data publicly accessible.

Data Fiduciary and Processing Personal Data.

"Data Fiduciary" (herein after 'Fiduciary') refers to any person or entity that, on its own or in collaboration with others, determines the objective and methods for handling personal data [section 2(i)]. The word "person" means various entities, including: (i) an individual, (ii) a Hindu undivided family, (iii) a company, (iv) a firm, (v) an association of individuals or a group, whether legally established or not, (vi) the State, and (vii) any other artificial legal entity not covered by the preceding sub-clauses [section 2(s)]. A Fiduciary (which refers to an individual or entity) is authorized to process a principal's personal information exclusively in compliance with the stated Act, and for a 'lawful purpose' and for certain 'legitimate use'. Such a purpose may involve the principal's granted consent or specific valid uses. The term "lawful purpose" denotes any objective that is not explicitly prohibited by legal statutes [section 4]. The term "certain legitimate uses" pertains to the intentions described in section 7.

The term "processing" concerning personal data pertains to wholly or partially automated actions or a set of actions executed on digital personal data. This includes tasks such as gathering, recording, arranging, organizing, storing, modifying, retrieving, utilizing, aligning, combining, indexing, sharing, transmitting through disclosure, disseminating, or otherwise facilitating access, imposing restrictions, erasing, or obliterating as described in section 2(x).

Section 7 enumerates the various contexts in which a Data Fiduciary can process personal data while adhering to the stipulated guidelines and circumstances laid out in the Act. The permissible purposes under section 7 are as follows:

(a) A Fiduciary is allowed to process the personal data of a Principal for a particular purpose for which the Data Principal has voluntarily provided her personal data to the Fiduciary. This is permissible unless the principal has explicitly indicated her non-consent for such usage.

(b) Processing by the State or its instrumentalities is permitted to offer subsidies, benefits, services, certificates, licenses, or permits as specified by regulations. This is applicable when: (i) The Principal has previously consented to such processing by the State or its instrumentalities for the mentioned purposes; or (ii) The personal data is available in digital or non-digital form in a database maintained by the State or its instrumentalities and adheres to the processing standards set by the Central Government's policy or any prevailing law.

(c)Processing is allowed for functions performed by the State or its instrumentalities according to Indian laws or in the interest of India's sovereignty, integrity, or security.

(d) Fiduciaries can process personal data to fulfill obligations under Indian laws that require disclosing information to the State or its instrumentalities, as long as the processing complies with disclosure provisions in other relevant laws.

(e) Processing is permitted to comply with judgments, decrees, orders, or claims, either under Indian laws or laws outside India, related to contractual or civil matters.

(f) Personal data can be processed to address medical emergencies posing threats to the Data Principal's life or immediate health, or the health of others.

(g) Processing is permissible to provide medical treatment or health services during epidemics, disease outbreaks, or other threats to public health.

(h) Fiduciaries can process personal data to ensure safety, provide assistance, or deliver services during disasters or instances of public order disruption.

(i) Processing for employment-related purposes or activities aimed at protecting employers from loss or liability, such as preventing corporate espionage, maintaining the confidentiality of trade secrets, intellectual property, classified information, or providing services or benefits sought by Data Principals who are employees.

If the legality of processing personal data relies on the principal's consent and such a matter arises in a proceeding, the Fiduciary is responsible for proving that a notice was presented to the principal and consent was acquired according to the provisions of this Act and its associated rules.

Notice to Principal

In accordance with section 5, whenever a fiduciary seeks consent from a Principal, as required by section 6, the Fiduciary must provide a notice to the Data Principal either before or alongside the consent request. This notice from the Fiduciary to the Principal must convey information about the specific personal data that is intended to be processed, the purpose for which this data will be used, instructions on how the principal can exercise their rights, and guidelines on how the principal can file a complaint with the Board. The manner and format of this notice will be prescribed by rules to be made.

In cases where a principal has already granted consent for their personal data to be processed prior to the commencement of this Act, the Fiduciary is obliged to, as soon as possible, furnish the principal with a notice. This notice must encompass (i) the specific personal data that has been processed and its purpose, (ii) information about how the principal can exercise their rights, and (iii) guidance on the procedure for the principal to lodge a complaint with the Board. During this period, the Fiduciary is allowed to continue processing the personal data unless the principal decides to withdraw their consent. Moreover, it is mandated that the Fiduciary must offer the principal the choice to receive the notice's content in English or any language specified in the Eighth Schedule to the Constitution.

Fair Consent of the Principal

All requests for consent under these provisions should be communicated to the principal by the fiduciary, using clear and straightforward language. Consent granted by the principal must be voluntary, specific, knowledgeable, unwavering, and unmistakable, involving a clear and affirmative action. This consent indicates an agreement to process their personal data for a precise purpose, limited only to the necessary personal data required for that particular purpose. Any aspect of consent that contradicts these guidelines or any prevailing laws will be null and void to the extent of the infringement. The principal should have the choice to access these requests and be provided with the contact details of a Data Protection Officer (DPO) or any other authorized individual to address their queries related to their rights under this Act.

When the principal's consent forms the basis for processing personal data, she has the right to revoke this consent at any time, with the process of withdrawal being as simple as the initial consent process. The principal will bear the consequences of this withdrawal, and it will not impact the legality of data processing conducted based on consent prior to its withdrawal. In the event that a principal retracts their consent for personal data processing, the fiduciary must promptly cease processing and ensure that any Data Processors they utilize also stop processing the principal's personal data. However, exceptions may apply if processing without consent is mandated or authorised by prevailing laws in India.

The principal can provide, oversee, assess, or withdraw consent using a "Consent Manager", which refers to an entity registered with the Board, serving as a central point of contact to facilitate principals in giving, managing, reviewing, and withdrawing consent through a transparent, accessible, and interoperable platform. The Consent Manager is accountable to the principal and operates according to prescribed obligations. Every Consent Manager must be registered with the Board based on stipulated conditions encompassing technical, operational, financial, and other aspects.

General obligations of Data Fiduciary

The General Responsibilities of a Data Fiduciary under Section 8 of the legislation are outlined as follows:

1. A Data Fiduciary is accountable for adhering to these provisions concerning any data processing conducted by itself or on its behalf by a Data Processor.
2. A Data Fiduciary can involve a Data Processor to handle personal data on its behalf, solely for activities linked to providing goods or services to Data Principals, subject to a valid contract.
3. If personal data processed by a Data Fiduciary is likely to influence a decision affecting the Data Principal or to be disclosed to another Data Fiduciary, the processing entity must ensure accuracy, consistency, and completeness of such data.

4. The Data Fiduciary is obliged to establish appropriate technical and organizational measures to effectively follow these provisions.
5. The Data Fiduciary must safeguard personal data under its control or possession, including data processed by a Data Processor, by employing reasonable security measures to prevent data breaches.
6. In the event of a personal data breach, the Data Fiduciary is required to notify the relevant authority and the affected Data Principals, according to the prescribed manner.
7. Unless retaining data is essential for legal compliance, the Data Fiduciary should erase personal data when the Data Principal withdraws consent or when the specified purpose is no longer being served, whichever occurs earlier. The Data Fiduciary should ensure that its Data Processor erases the data too.
8. The purpose mentioned in clause (a) of subsection (7) is deemed no longer in effect if the Data Principal does not engage the Data Fiduciary for the intended purpose or exercise her processing-related rights within the prescribed time frame.
9. If applicable, a Data Fiduciary should publish the business contact details of a Data Protection Officer or a representative who can address Data Principals' queries regarding personal data processing.
10. The Data Fiduciary should establish an efficient mechanism to resolve Data Principals' complaints.
11. For the context of this section, a Data Principal is considered not to have approached the Data Fiduciary for a specific purpose during periods when she has not initiated contact with the Data Fiduciary, either personally or through electronic or physical communication.

Significant Data Fiduciaries

The term "Significant Data Fiduciary" refers to any Fiduciary or a group of Data Fiduciaries designated by the Central Government according to section 10 [section 2(z)]. Additional responsibilities of Significant Data Fiduciaries are outlined in section 10.

The Central Government holds the authority to classify specific Data Fiduciaries or categories of Data Fiduciaries as Significant Data Fiduciaries, based on an evaluation of various relevant factors. These factors include: (a) the extent and sensitivity of personal data being processed, (b) potential risks to the rights of Data Principals, (c) potential impact on India's sovereignty and integrity, (d) potential risks to electoral democracy, (e) implications for national security, and (f) effects on public order.

Significant Data Fiduciaries are required to: (a) designate a Data Protection Officer who will (i) represent the Significant Data Fiduciary under the provisions, (ii) be situated in India, (iii) be an individual accountable to the Board of Directors or a similar governing body of the Significant Data Fiduciary, and (iv) serve as the contact point for the grievance resolution system outlined in these provisions. (b) engage an independent data auditor to conduct data audits, assessing the compliance of the Significant Data Fiduciary in accordance with these provisions. (c) undertake the following additional measures: (i) periodic Data Protection Impact Assessment, involving defining Data Principals' rights and the purpose of processing their personal data, evaluating and managing risks to Data Principals' rights, and addressing other relevant aspects as prescribed, (ii) regular audits, and (iii) any other measures consistent with the stipulations of this Act, as prescribed.

Rights and Duties of Data Principal

When a Fiduciary intends to process personal data of a child or a disabled person under the care of a legal guardian, they must secure consent from the parent or guardian in the manner prescribed by section 9. The term "consent of the parent" in this context also encompasses consent from the lawful guardian, if applicable. A Fiduciary is prohibited from engaging in any data processing that could potentially harm a child's well-being. This includes refraining from tracking, monitoring behaviour, or delivering targeted advertisements to children. However, these provisions might not apply to the processing of personal data of a child by specific classes of Fiduciaries or for specific purposes, subject to the conditions prescribed by the Act. If the Central Government is satisfied that a Fiduciary has implemented verifiably safe data processing practices for children's personal data, the government can issue a notification specifying the age beyond which that Fiduciary will be exempt from certain obligations related to data processing.

The principal has the entitlement to request certain information from a Fiduciary, to whom they've granted prior consent for personal data processing, as specified in section 7(a). Upon making a request in the prescribed manner, the Principal can ask for: (a) a summary of the personal data being processed by the Data Fiduciary and the related processing activities, (b) details of all other Data Fiduciaries and Data Processors with whom the data has been shared, including a description of the shared data, and (c) any additional information pertaining to the personal data and its processing, as prescribed. However, the provisions of clause (b) and (c) above do not apply when the Data Fiduciary shares personal data with another Data Fiduciary authorized by law to access such data. This applies when the sharing is a result of a written request made by the other Data Fiduciary for the purpose of preventing, detecting, investigating offenses or cyber incidents, or for the prosecution or punishment of offenses.

An individual who is referred to as a Principal possesses the entitlement to rectify, supplement, update, and delete their personal information that was previously given approval for processing, which includes approval as defined in clause (a) of section 7. This right adheres to any current legal requirements or procedures. In response to a request for rectification, supplementation, or updating from a Principal, a Fiduciary is obligated to: (a) rectify any inaccurate or deceptive personal information, (b) complete any incomplete personal information, and (c) update the personal information. For the purpose of erasing their personal information, a Data Principal needs to submit a request as per the prescribed manner to the Data Fiduciary. Upon receiving such a request, the Data Fiduciary is required to delete the personal information unless its retention is necessary for the designated purpose or for compliance with prevailing legal requirements [section 12].

A Principal possesses the entitlement to accessible avenues for addressing complaints, which must be provided by a Fiduciary or Consent Manager. These avenues pertain to any action or inaction of the mentioned Data Fiduciary or Consent Manager in connection with fulfilling their responsibilities regarding the personal data of the principal or facilitating her rights under these stipulations. The Fiduciary or Consent Manager is obligated to reply to grievances within a timeframe defined by regulations, commencing from the date of receipt. This requirement is applicable to all Fiduciaries or a specified category of them.

Prior to approaching the Board, the Data Principal should explore the option of resolving her complaint through the mechanisms outlined in this section. [section 13]. A Principal possesses the entitlement to appoint, following the prescribed procedure, another person who, in case of the Data Principal's demise

or inability, will carry out the Data Principal's rights in alignment with these rules to be made (as detailed in section 14).

The principal is tasked with fulfilling the following responsibilities: a) Adhere to the stipulations of all pertinent laws currently in effect when exercising rights under these clauses. b) Guarantee not to assume the identity of another individual when submitting personal data for a designated purpose. c) Guarantee not to withhold any crucial information while supplying personal data for any document, distinct identifier, official identification, or address validation issued by the State or any of its affiliated bodies. d) Guarantee not to submit a fraudulent or frivolous grievance or complaint to a Data Fiduciary or the Board. e) Provide solely information that can be validated as authentic while exercising the right to amend or erase under these provisions (section 15).

Exemptions from operations of the Act

Section 17 of the Act outlines instances where exemptions from its operations are granted. The Act's reach does not extend to the following scenarios: (a) Instances where processing personal data is essential for asserting legal rights or claims. (b) Processing conducted by courts, tribunals, or other authorized entities fulfilling judicial, regulatory, or supervisory roles. (c) Processing conducted to prevent, detect, investigate, or prosecute offenses. (d) Processing personal data of non-Indian residents based on contracts with foreign entities. (e) Processing related to court-approved business arrangements. (f) Processing aimed at evaluating the financial status of defaulters by financial institutions.

Exclusions from the Act encompass: (a) Processing by state instrumentalities in the interest of national welfare. (b) Activities involving research, archiving, or statistics that don't impact individual rights. (c) Specific Data Fiduciaries, such as startups, may qualify for exemptions.

Startups are private enterprises acknowledged as per government criteria. For state-related processing, certain sections might not apply. The Central Government holds the authority to exempt Fiduciaries from Act provisions and can extend these exemptions through notifications within five years of the Act's initiation.

Role of Data Processor

"Data Processor" refers to any individual who handles personal data on behalf of a Data Fiduciary as defined in section 2(k).

The Central Government reserves the right to, through notification, limit the transmission of personal data by a Data Fiduciary for processing to specific countries or territories beyond India, as indicated in section 16. This section's provisions do not hinder the relevance of any existing laws in India that presently enforce a higher level of protection or constraints on the transfer of personal data by a Data Fiduciary to foreign locations in connection with any personal data, specific Data Fiduciaries, or particular categories thereof.

Data Protection Board of India

Starting from the date chosen by the Central Government through an official notice, a Board known as the Data Protection Board of India (Board for brevity) will be established to fulfill the objectives of this Act (Section 18). The Board will possess everlasting continuation, and the authority, within the limits of this Act, to gain, possess, and relinquish assets, whether they are movable or immovable. The Board also holds the right to engage in contracts and to initiate legal actions. The Board will comprise a

Chairperson and a specific number of additional Members, as decided by the Central Government (Section 19). The individuals possessing qualities of competence, honesty, and influence, along with specialized knowledge or practical experience in various domains such as data management, law enforcement, social or consumer protection laws, conflict resolution, information technology, digital economy, legal matters, regulations, or related areas that the Central Government deems valuable for the Board's functioning are appointed. The compensation and Tenure The pay, perks, and work arrangements are to be determined according to official rules to be made. Both the Chairperson and Members will serve for a period of two years, with the option to be reappointed. A person cannot be appointed or remain as the Chairperson or a Member under following circumstances: (a) being declared insolvent, (b) being convicted of an offense involving serious moral wrongdoing according to the Central Government's view, (c) being physically or mentally unfit for the role, (d) having financial or other interests that could negatively impact their duties, or (e) misusing their position to the detriment of public interest. The Chairperson or Member cannot be dismissed by the Central Government without being given a chance to present their perspective on the matter.

Powers and Responsibilities of Board

As mandated in the Act, the Board is empowered to exercise and execute the tasks relating to protection of personal data in the instances of breaches on the part of fiduciary are noticed. "Personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability {section 2(u)] of personal data. Section 27 of the Act assogns the following responsibilities to the Board.

(a) Upon receipt of a notification regarding a personal data breach in accordance with section 8, subsection (6), the Board is authorized to issue immediate corrective or mitigative actions if a personal data breach occurs. Furthermore, it holds the authority to investigate such breaches and levy penalties as outlined in this Act.

(b) In instances where a principal files a complaint concerning a personal data breach, a violation of a Fiduciary's obligations related to their personal data or the exercise of their rights as per the Act's provisions, or when referred by the Central Government, State Government, or under court directives, the Board is empowered to investigate such breaches and impose penalties as per the Act.

(c) If a Data Principal raises a complaint about a violation of obligations concerning personal data by a Consent Manager, the Board is entitled to investigate the breach and impose penalties as specified in this Act.

(d) Upon receiving notification of a breach of any registration condition of a Consent Manager, the Board is authorized to investigate the breach and apply penalties as defined in this Act.

(e) When the Central Government refers a breach of provisions outlined in section 37, subsection (2), committed by an intermediary, the Board has the authority to investigate the breach and levy penalties as specified in this Act.

For the efficient execution of its responsibilities as per the Act's provisions, the Board can issue necessary directives to individuals after affording them an opportunity to present their case and after

documenting reasons in writing. These directives must be complied with by the concerned individuals. The Board also possesses the ability to alter, suspend, rescind, or revoke issued directives based on a representation from an affected individual or a reference made by the Central Government. In doing so, the Board can impose certain conditions as deemed appropriate, which will govern the effect of such modifications, suspensions, rescissions, or revocations.

The Board is to function as an independent entity, aiming to operate predominantly in a digital capacity. The process of receiving complaints, assigning cases, conducting hearings, and delivering verdicts shall be designed to be digitally streamlined. The Board is to incorporate technological and legal measures as mandated to form a 'digital office' as defined under section 2 (*m*) of the Act. The digital office means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode. Upon receiving notifications, complaints, references, or directives as outlined in subsection (1) of section 27, the Board is empowered to take actions in alignment with the stipulations of this Act and the corresponding rules. The Board is responsible for assessing whether sufficient grounds exist to initiate an inquiry. Should the Board find insufficient grounds, it reserves the authority, with the rationale duly documented, to conclude the proceedings.

However, if the Board identifies adequate grounds warranting an inquiry, it possesses the prerogative, with reasons recorded in writing, to delve into the affairs of an individual or entity. The purpose of such an inquiry is to ascertain compliance with, or adherence to, the provisions outlined in this Act. The Board is mandated to conduct these inquiries while adhering to the principles of natural justice. During the course of such inquiries, the Board is required to document the rationales behind its actions. For the effective discharge of its responsibilities under this Act, the Board is vested with powers analogous to those of a civil court under the Code of Civil Procedure, 1908. These powers include:

(a) Summons and enforcing attendance of individuals for examination under oath. (b) Acceptance of evidence in the form of affidavits, with the ability to demand the disclosure and production of pertinent documents. (c) Inspection of data, records, documents, registers, accounting records, and other relevant materials. (d) Any other matters deemed necessary and prescribed.

The Board and its officials are not authorized to obstruct access to premises or seize any equipment or items that might disrupt the regular operations of an individual or entity. If deemed necessary, the Board can enlist the assistance of police officers or officers from the Central Government or State Government to aid its endeavours under this section. These officers are duty-bound to comply with such requisitions. While conducting an inquiry, if the Board deems it appropriate, it can issue interim orders, contingent upon providing the concerned party an opportunity to present their case and reasons documented in writing. Upon the culmination of the inquiry and affording the individual concerned an opportunity to be heard, the Board can, for reasons documented in writing, either terminate the proceedings or proceed in accordance with section 33. In instances where, at any stage subsequent to receiving a complaint, the Board perceives the complaint to be false or frivolous, it holds the power to issue a cautionary warning or levy costs on the complainant.

Penal Provisions

Following the conclusion of an inquiry, if the Board determines that an individual has significantly violated the provisions, it may, after affording the individual an opportunity to present their case, impose a monetary penalty as specified in the Schedule. The categories of provisions within this Act or its corresponding rules, along with the potential penalties outlined in the schedule, are as follows:

(1) In case of a breach in upholding the Data Fiduciary's obligation to implement reasonable security measures to safeguard personal data under subsection (5) of section 8, the penalty may range up to 250 crore rupees.

(2) If there is a breach in adhering to the obligation of notifying the Board or the affected Data Principal regarding a personal data breach under subsection (6) of section 8, the penalty may extend to 200 crore rupees.

(3) For a breach in fulfilling additional obligations concerning children under section 9, the penalty may extend up to 200 crore rupees.

(4) In case of a breach in fulfilling the extra obligations of a Significant Data Fiduciary under section 10, the penalty may extend up to 150 crore rupees.

(5) If there is a breach in upholding the duties outlined in section 15, the penalty may extend to 10,000 rupees.

(6) In instances of a breach of any term within voluntary undertaking accepted by the Board under section 32, the penalty will be determined based on the extent applicable for the specific breach for which proceedings under section 28 were initiated.

(7) For violating any other provision outlined in this Act or the corresponding rules, the penalty may extend to 50 crore rupees.

To ascertain the appropriate amount of the monetary penalty to be imposed, the Board should consider the following factors:

(a) The nature, seriousness, and duration of the breach. (b) The type and sensitivity of the personal data impacted by the breach. (c) Whether the breach has occurred repeatedly. (d) Whether the individual gained any advantage or avoided any losses as a result of the breach. (e) Whether the individual took action to mitigate the effects and consequences of the breach, and the promptness and effectiveness of such measures. (f) The proportionality and effectiveness of the proposed monetary penalty, considering the necessity to ensure compliance with the Act's provisions and to discourage breaches. (g) The probable impact of imposing the monetary penalty on the individual. For the purposes of this act, the term 'gain' and 'loss' are defined as follows:

"(i)Section 2 (o) "gain" means- (i) a gain in property or supply of services, whether temporary or permanent; or (ii) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration.

(ii) Section 2 (p) "loss" means- (i) a loss in property or interruption in supply of services, whether temporary or permanent; or (ii) a loss of opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration".

All funds collected as penalties levied by the Board under this Act will be deposited into the Consolidated Fund of India. [Section 34]. The Central Government, the Board, its Chairperson, Members, officers, or employees are immune from legal actions arising from actions taken in good faith under this Act or its rules. (Section 35).

After giving the Data Fiduciary an opportunity to present their case, if it's deemed necessary or beneficial for the public interest, the Central Government can order an agency or intermediary to block public access to such information through a written and recorded justification. Any intermediary

receiving such an order must comply. [Section 37]. Civil courts cannot handle suits related to matters within the Board's authority as per this Act. No court or authority can grant injunctions against actions taken or to be taken under this Act's provisions. (Section 39). The act has provisions relating to Appeal to Appellate Tribunal, Alternate dispute resolution, Power to make rules, Power to amend Schedule, to remove difficulties and amend certain acts.

The Way Forward

The introduction and enactment of the Digital Personal Data Protection Act (DPDPA) in 2023 mark a significant milestone in India's journey toward safeguarding individuals' digital personal data while nurturing innovation and economic growth. As the nation embarks on the path to implementing this pivotal legislation, several strategic steps and considerations are poised to shape the way ahead.

1. One of the initial steps involves the establishment of a robust legal framework and digital office to be able to perform all activities online.
2. The creation of a Board with dedicated members for overseeing and enforcing the provisions of the DPDPA is essential. This entity should possess the necessary technical expertise and resources to ensure effective compliance and enforcement across industries.
3. successful implementation of the DPDPA necessitates awareness and understanding among individuals, businesses, and other stakeholders. Extensive awareness campaigns and educational initiatives should be conducted to elucidate the rights and responsibilities enshrined in the Act. Workshops, training sessions, and guidelines for businesses on complying with data protection standards can help build capacity and facilitate smoother adaptation.
4. Different industries handle personal data in distinct ways. Developing industry-specific guidelines that align with the Act's principles can offer tailored solutions to address unique challenges. These guidelines can serve as practical tools for businesses to interpret and implement the Act's provisions in their specific contexts.
5. The concept of "privacy by design and default" is central to the Act's ethos. Integrating privacy considerations into the design of products, services, and systems from the outset is crucial. Businesses should prioritize data minimization, user consent mechanisms, and data protection measures to ensure compliance at every stage of development.
6. The Act includes provisions regulating cross-border data transfers. Formulating mechanisms for secure cross-border data flows while adhering to international data protection standards requires strategic collaborations with other countries and organizations. Implementing adequate safeguards such as standard contractual clauses or obtaining regulatory approvals for such transfers will be pivotal.
7. Regular audits and reporting mechanisms should be established to assess compliance and track the Act's effectiveness. These audits can help identify gaps, areas for improvement, and instances of non-compliance, thereby ensuring a continuous cycle of enhancement in data protection practices.
8. The Act's provisions related to remedies and redress mechanisms should be efficiently established. Individuals must have accessible avenues to exercise their rights and seek remedies in case of data breaches or privacy violations.
9. The landscape of technology and data processing is ever evolving. The Act should be reviewed periodically to ensure its relevance and effectiveness in addressing emerging challenges.

The implementation of the Indian DPDPA, 2023, is a dynamic and intricate process that requires strategic planning, collaboration, and continuous vigilance. By adopting a comprehensive approach that encompasses regulatory measures, awareness-building, technological advancements, and industry

collaboration, India can successfully navigate the road ahead to ensure the protection of individuals' digital personal data in a rapidly evolving digital landscape.

Mr. M.G.Kodandaram, IRS.
Assistant Director (Retd)
ADVOCATE and CONSULTANT