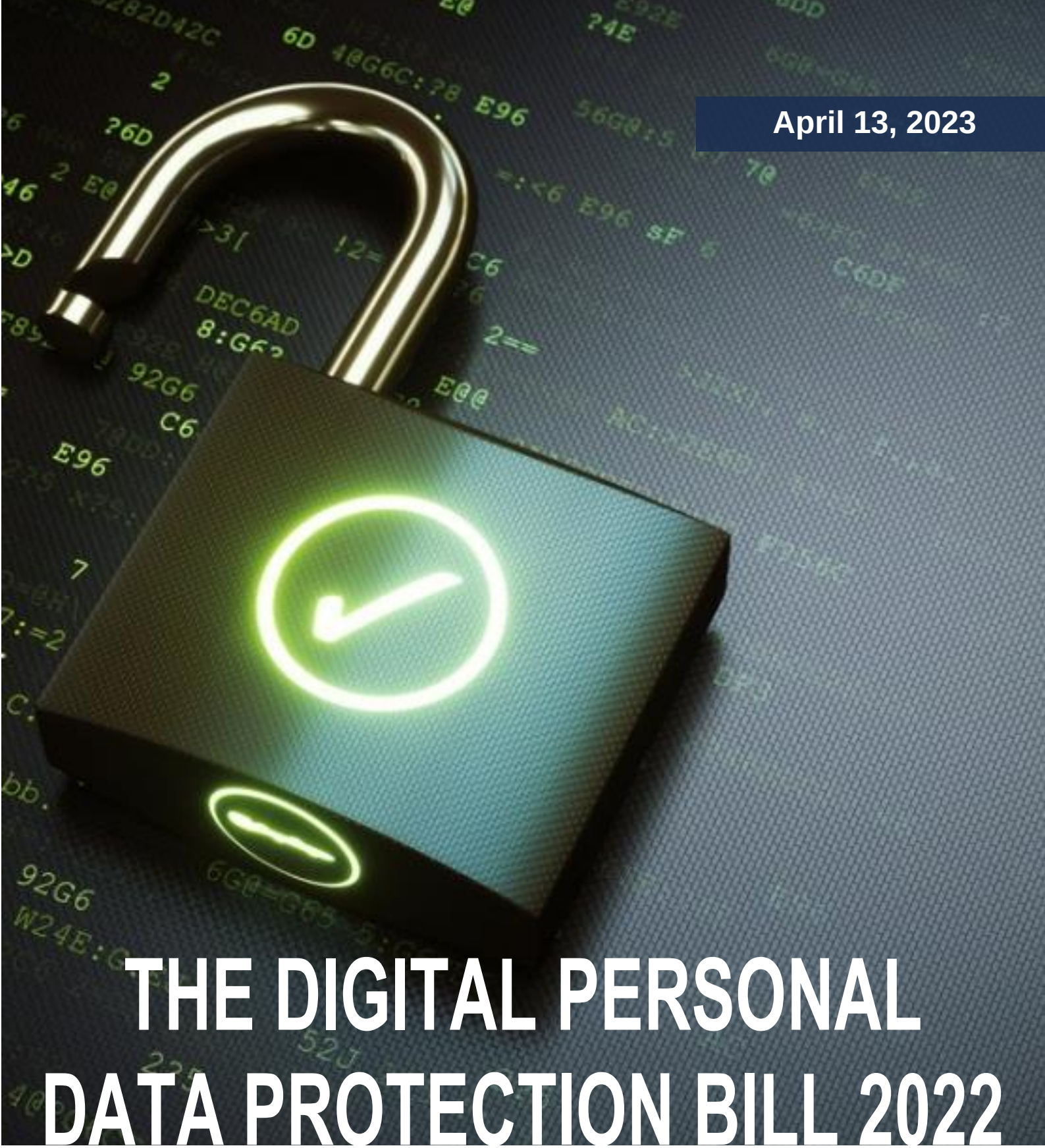

April 13, 2023

THE DIGITAL PERSONAL DATA PROTECTION BILL 2022

- An Analysis

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

1. Introduction

The draft Digital Personal Data Protection Bill, 2022 ("**DPDPB**") was released on November 18, 2022 by the Ministry of Electronics and Information Technology ("**MeitY**") for public consultation, pursuant to its withdrawal of the draft Personal Data Protection Bill 2019 ("**PDPB 2019**") in August 2022. MeitY has significantly altered the framework of DPDPB compared to the PDPB 2019, though there are important aspects that MeitY has sidestepped.

Meanwhile, one of the most concerning issues with DPDPB is the fact that the provisions cover a basic framework for data protection and privacy, leaving it largely for the Central Government to assess and notify further protections at a later stage, as and when deemed necessary. This not only puts the ambit of governmental scrutiny with a wider reach but also prevents adequate protection of fundamental rights to privacy and protection.

This paper provides an overview of the provisions of DPDPB and analyses its impact.

2. Key Definitions

Before looking into the intricacies of DPDPB and examining its applicability and exceptions, it is pertinent to note the definitions of certain key terms:

(i) **Data:** Data is defined as a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means.

(ii) **Personal Data**: It is defined as the Data concerning an individual who is identifiable by or in relation to such data. Thus, not only Data that simply identifies an individual but also such Data which "relates to" or concerns with an individual in some manner, will be classified as Personal Data. It is interesting to note that the definition of Personal Data is not restricted to factual information about an individual but covers 'opinions' and 'inferences' as well if the individual can be identified from such data, either directly or indirectly.

(iii) **Data Principal**: The individuals to whom the Personal Data relates are called "**Data Principals**". In case of a child, i.e., an individual who is below 18 years, his parents or lawful guardian will be regarded as Data Principals. Thus, a child's Personal Data may be shared by his parents or a local guardian.

(iv) **Data Fiduciary**: Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data is a "**Data Fiduciary**". Impliedly, in respect of a particular set of Personal Data, there can be more than one Data Fiduciary, i.e., when more than one person decides the purpose and means of processing of Personal Data. This is similar to the concept of "Data Controller" under the General Data Protection Regulations ("**GDPR**"), though not elaborated under DPDPB.

(v) **Processing:** It means automated operations or set of operations performed on Personal Data, and may include operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction. To simplify, it refers to one or more operations on the Personal Data that is automated through the use of computers and computer software.

3. Scope

3.1. Exclusion of non-digital data:

3.1.1. Section 4 of DPDPB states that DPDPB applies only to the “processing of digital personal data”. Though the term ‘personal data’ is defined by DPDPB, the phrase “digital personal data” is not defined. However, Section 4 of DPDPB qualifies the phrase “digital personal data” with the requirement that such personal data should, either be collected from Data Principals online or, if collected offline, be digitized. For good measure, Section 4(3)(b) of DPDPB states that it shall not apply to offline personal data.

3.1.2. Exclusion of non-digital data will have the impact of excluding vast swathes of personal data which is not in electronic form. It would also allow commercial players to collect personal data in non-digital form without having to comply with DPDPB. However, on the flip side, in this day and age, it would pose a logistical challenge to store large quantities of personal data on paper, without scanning it into an electronic format.

3.2. Extra-territorial application

3.2.1. Section 4 of DPDPB states that the bill will apply outside India only to digital personal data that is processed outside India, provided such processing is in connection with any profiling of, or activity of offering goods or services to data principals within India. The PDPB 2019 had provided that it would apply to the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is (i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India or (ii) in connection with any activity which involves profiling of data principals within the territory of India.

3.2.2. Therefore, there are two crucial differences between DPDPB and the PDPB 2019. The latter applied to the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is in connection with any business carried on in India, even if the data principals involved are not based in India. PDPB 2019 applies to the processing of personal data if it is in connection with the “systematic activity” of offering goods or services to data principals within the territory of India. Under DPDPB, the activity of offering goods or services to data principals within the territory of India need not be “systematic”.

3.3. Exclusion of non-automated processing of personal data

3.3.1. Section 4(3)(a) of DPDPB provides that it shall not apply to the processing of personal data if the processing is non-automated. Thus, even if personal data is digital or has been digitized, after having been collected offline, DPDPB shall not apply to the processing of such personal data if the processing is non-automated. DPDPB has defined the term “automated” to mean any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data.

3.3.2. The PDPB 2019 defined “automated” in a manner substantially similar to DPDPB. Under the PDPB 2019 "automated means" meant any equipment capable of operating automatically in response to instructions given for the purpose of processing data. However, the PDPB 2019 did not exempt the processing of personal data through non-automated means from its scope, save in the case of small entities who were exempt from certain provisions of the PDPB 2019, such as

provisions relating to requirement of notice for collection or processing of personal data, quality of personal data processed, restriction on retention of personal data, right to data portability, the right to be forgotten, general conditions for the exercise of rights by data principals, transparency and accountability measures, privacy by design policy, transparency in processing of personal data, security safeguards, reporting of personal data breach, classification of data fiduciaries as significant data fiduciaries, data protection impact assessment, maintenance of records, audit of policies and conduct of processing the requirement to appoint a data protection officer, the requirement to have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner. A "small entity" was defined to mean a data fiduciary which would be classified as such by the data protection authority (sought to be established under the PDPB 2019) on the basis of its turnover in the preceding financial year, the purpose for which it collected personal data and the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.

3.3.3. PDPB 2019 required that if a data principal processes personal data through automated means, the data principal shall have the right to receive:

(i) the personal data provided to the data fiduciary;
(ii) the data which was generated in the course of provision of services or use of goods by the data fiduciary; and
(iii) the data which forms part of any profile on the data principal or which the data fiduciary has otherwise obtained, in a structured, commonly used and machine-readable format.

3.4. Personal or domestic purpose exclusion

3.4.1. Section 4(3)(c) of DPDPB provides that DPDPB shall not apply to any personal data processed by an individual for any personal or domestic purpose.

3.4.2. PDPB 2019 had also kept outside its scope any personal data that is processed by a natural person for any personal or domestic purpose. However, this exemption was subject to an exception for which the processing involves disclosure to the public or is undertaken in connection with any professional or commercial activity. DPDPB does not contain any such exception for data process which, though carried out for any personal or domestic purpose, involves disclosure to the public, or is undertaken in connection with any professional or commercial activity.

3.5. Ancient data exclusion

3.5.1. Section 4(3)(d) of DPDPB provides that DPDPB shall not apply to any personal data that is contained in a record that has been in existence for at least 100 years. This exclusion was neither found in any of the previous data privacy bills nor in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. It is unclear what the objective of this exclusion is, since non-digital data is already exempt and most 100-year-old data would be non-digital, unless it is of antique value and has been digitized. If a museum digitizes letters written by Indian soldiers (to their families) serving in the British Indian army during the First World War, would such letters be exempt, even if they contain the personal data of the soldiers who wrote those letters? On a plain reading of Section 4(3)(d) of DPDPB, such digitized letters would not be exempt since Section 4(3)(d) requires the personal data to be contained in a record that has been in existence for at least 100 years. DPDPB does not define the term "record", but here "record" would refer to the digital version of the letters. However,

if the letters themselves can be considered as the "record", such letters would be exempt even if they have been digitized. Since non-digital data is already outside the scope of DPDPB, the latter interpretation may be the only viable one.

4. No special Protection for Sensitive Personal Data or Critical Personal Data

DPDPB treats all personal data alike and does not afford any special protection for sensitive personal data or critical personal data.

4.1. Sensitive Personal Data

4.1.1. Section 43A of the IT Act 2000 refers only to 'sensitive personal data or information', giving the impression that the 2011 Rules are meant to deal only with sensitive personal data and would not apply to non-sensitive personal data. However, the 2011 Rules uses the phrase 'personal information or sensitive personal data or Information' in a few instances, though the phrase 'sensitive personal data or information' is a lot more common.

The 2011 Rules lists the following six types of personal data as sensitive personal data:

(i) password;
(ii) financial information such as bank account or credit card or debit card or other payment instrument details;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history; and
(vi) biometric information;

In addition to the above, any detail or any information relating to the above six types of sensitive personal data as provided to a body corporate for providing services or for the processing of data under a lawful contract would also be sensitive personal data.

Passwords were not considered to be sensitive personal data under the PDPB 2019, though the Personal Data Protection Bill, 2018 had included passwords in the list of sensitive personal data. Other than passwords, all other categories of sensitive personal data provided for in the 2011 Rules were covered by the definition of sensitive personal data given in the PDPB 2019. Instead of 'medical records and history' and 'physical, physiological and mental health condition', PDPB 2019 had 'health data'. PDPB 2019 also had the following additional categories of sensitive personal data, which are not found in the 2011 Rules, namely, health data, official identifier, sex life, genetic data, transgender status, intersex status, caste or tribe, and religious or political belief or affiliation.

4.1.2. Under the 2011 Rules, the obligation to obtain prior consent before collecting data, applies only to the collection of sensitive personal data, though prior to the collection of any personal data, the provider of personal data should be given the option to not to provide the personal data sought to be collected. Thus, it is possible to collect non-sensitive personal data without prior consent under the 2011 Rules. It is sufficient if the data principal is notified that his/her personal data is being collected, the purpose for which the personal data is being collected, the intended recipients of the information, and the name and address of the agency that is collecting the information and of the agency that will retain the information.

4.1.3. PDPB 2019 did not contain the stark distinction between sensitive and non-sensitive personal data which the 2011 Rules did. Unlike under the 2011 Rules, collection of personal data under the PDPB 2019 required the prior consent of the data principal, irrespective of whether the personal data was sensitive or not. However, PDPB 2019 did offer additional protection to sensitive personal data in a few crucial respects, such as:

(i) when obtaining consent for the processing of personal data, if the personal data is sensitive, the consent of the data principal should be explicitly obtained after informing the data principal of the purpose of, or operation in, processing which is likely to cause significant harm to the data principal. The consent also should be in clear terms without recourse to inference from conduct in a context. The data principal should also be given the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

(ii) the exceptions relating to the processing of personal data in connection with employment do not apply in the case of sensitive personal data; and

(iii) all sensitive personal data has to be stored in India and any transfer outside India is subject to a number of stringent conditions, such as cases where explicit consent is given by the data principal for such transfer or where the transfer is made pursuant to a contract or intra-group scheme approved by the data protection authority on the basis that, inter alia, such sensitive personal data shall be subject to an adequate level of protection in the transferee jurisdiction, having regard to the applicable laws and international agreements, and such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction.

4.2. Critical personal data

PDPB 2019 introduced the concept of critical personal data, though the exact meaning of the phrase was left to be prescribed by rules to be framed by the Central Government. Under PDPB 2019 and DPDPB, critical personal data cannot be transferred outside India. DPDPB does not mention critical personal data at all.

5. Grounds for processing digital personal data

Section 5 of DPDPB sets out three basic rules for the processing of personal data, namely that the processing has to be (i) in accordance with DPDPB, (ii) for a lawful purpose and (iii) for which the data principal has given or is deemed to have given his/her consent.

6. Consent

6.1. Under DPDPB, all processing of digital personal data by Data Fiduciaries is subject to obtaining the Data Principal's consent. DPDPB envisages consent mechanism as the primary safeguard to protect the rights of Data Principals.

6.2. Interestingly, DPDPB contemplates express as well as implied consent from the Data Principals. While express consent (under Section 7 of DPDPB) is preceded by a notice to the Data Principal and ought to be specific, unambiguous and informed, deemed consent (under

Section 8) requires no such notice to the Data Principal, is based on the principle of necessity, and is restricted to limited scenarios contained in Section 8 of DPDPB.

6.3. For the processing of personal data of a child under the age of 18 years, express consent ought to be taken from a parent/ legal guardian and the same should be *verifiable* – thereby creating a higher threshold of compliance for the Data Fiduciary.

6.4. This section does a detailed analysis of the requirement of obtaining "consent" for processing of data under DPDPB. The key features are detailed below:

(i) **Informed Consent**: DPDPB states that consent[1] given by the Data Principal should be *free, specific, informed and unambiguous* and such consent should be given by a *clear affirmative action* which signifies an agreement to processing personal data for a specified purpose. Further, for consent to be given under Section 7, the Data Fiduciary must give a notice[2] to the Data Principal. The said notice has to be itemized and must contain in clear and plain language (i) the description of the data sought; and (ii) purpose for processing such data.

By focusing on informed consent, DPDPB aims to fill the existing void of information asymmetry where previously, the Data Principal may not be aware about the extent to which her personal data was being used or processed. There is a further requirement of furnishing contact details of a Data Protection Officer or an authorized person of the Data Fiduciary[3] as part of notice. This reflects the legislature's intent is to ensure transparency and empower the Data Principal by providing a convenient and ready grievance redressal mechanism.

While DPDPB lays down detailed parameters for express consent, there is no guidance on what would constitute or free, specific, informed and unambiguous consent, or any precise definitions thereof. Further, DPDPB fails to enumerate what is "clear and plain language" in a notice. The parameters governing express consent are rather subjective and overly broad.

(ii) **Right to Withdraw Consent**: DPDPB allows the Data Principal to withdraw her consent *at any time*[4]. It further mandates the Data Fiduciary to ensure that the process for withdrawal is as easy as the one for giving consent. This ensures that there are no complicated or long procedural requirements for withdrawal of consent by the Data Principal.

(iii) **Effect of Withdrawal of Consent**: On withdrawal of consent for processing of personal data by the Data Principal, the Data Fiduciary and its Data Processors must cease processing the personal data of the Data Principal. This must be done within a *reasonable period*[5]. While DPDPB does not define or provide any contours for what would constitute "reasonable period", it will be interesting to see how this provision is interpreted especially for significant data fiduciaries Significant Data Fiduciary ("**SDF**") handling and processing large volumes of personal data.

[1] Section 7, Digital Personal Data Protection Bill, 2022.
[2] Section 6, Digital Personal Data Protection Bill, 2022.
[3] Section 7(3), Digital Personal Data Protection Bill, 2022.
[4] Section 7(4), Digital Personal Data Protection Bill, 2022.
[5] Section 7(5), Digital Personal Data Protection Bill, 2022.

(iv) **Role of a Consent Manager**: For the purpose of managing "consent" of the Data Principal, DPDPB envisages that a Data Fiduciary may engage the services of a "consent manager" – an entity that must register itself with the Data Protection Board of India ("**Board**"), the regulatory body being created under DPDPB. A consent manager is accountable to the Data Principal and acts on its behalf to give, manage, review or withdraw consent[6]. Under DPDPB, a consent manager is also deemed to be a Data Fiduciary.

(v) **Burden of Proof on Data Fiduciary**: In any proceedings for non-compliance with provisions of DPDPB, the onus of proof is on the Data Fiduciary to demonstrate that (a) a notice was given by it to the Data Principal; and (b) consent was obtained in accordance with provisions of DPDPB.

6.5. However, Section 8 of DPDPB entails certain events, wherein a Data Principal may not give affirmative action and may act in a manner wherein he/ she will be deemed to have given consent to a Data Fiduciary for processing his/ her Personal Data. MeitY states that in such events, seeking consent of Data Principal is impracticable or inadvisable due to pressing concerns This has also been elaborated in the explanatory note to DPDPB that had been published by MeitY, which explains deemed consent to apply in "*clearly defined situations wherein insisting on consent would be counterproductive*".[7]

6.6. In a situation where a Data Principal would voluntarily provide their Personal Data, consent would be deemed to be given; however, it must be reasonably expected of such Data Principal to provide their consent. Deemed consent would apply, *inter-alia*, in the following cases where the processing of Personal Data is necessary:

(i) For the performance of any laws, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State;
(ii) Compliance with any judgment or order issued under law;
(iii) Taking measures to ensure medical treatment and ensure safety in case of threat to life or immediate threat to the health of any individual during an epidemic or any other threat to public health;
(iv) In the interests of the general public, such as, prevention of fraud, network and information security, credit scoring, debt recovery, in case of mergers, acquisitions or any other similar combination or corporate restructuring, for the purposes related to the employment, maintenance of confidentiality of intellectual property;
(v) For any fair and reasonable purpose after considering any public interest in such processing, whether the legitimate interests for such processing outweigh any adverse effect on the rights of the Data Principal, and reasonable expectations of the Data Principal; and
(vi) For the purposes related to employment, including maintenance of confidentiality recruitment, termination of employment, etc.

6.7. While PDPB, 2019 states explicit scenarios wherein the Personal Data of employees could be processed, DPDPB makes use of a non-exhaustive proviso when it uses the word "including".

[6] Section 7(7), Digital Personal Data Protection Bill, 2022.
[7] Explanatory Note – The Digital Personal Data Protection Bill, 2022.

Similarly, unlike PDPB 2019, deemed consent for public interest under DPDPB also incorporates a non-exhaustive *proviso*.

6.8. Further, PDPB, 2019 limited the processing of Personal Data by an employer only to non-sensitive personal data, however, as noted above DPDPB does not distinguish between sensitive and non-sensitive data, thereby permitting Data Fiduciaries a wider ambit with respect to the Personal Data of their Data.

6.9. The concept of deemed consent is derived from the data protection laws of Singapore and is similar to PDPB, 2019 which set out 'reasonable purposes' for Data Fiduciaries to process Personal Data without the consent of the Data Principal. However, PDPB 2019 was a step ahead in that it prescribed a mechanism for enactment of rules and regulations for 'reasonable purposes' considering that there is a window for such a broad consent to be misused by Data Fiduciaries. Such mechanism is absent in DPDPB.

6.10. Under DPDPB, there is no requirement to provide prior or post-facto notice to the Data Principal in case of deemed consent. Consequently, Data Principals may not have any information on what, why, how and when their Personal Data was processed, and this dilutes the significance of notice and consent under Section 6 and Section 7 of DPDPB, respectively. The said section is an area of concern as Data Principals may not have a recourse against Data Fiduciaries due to the absence of requirement of notice, which leads to lack of safeguards and does not carry the qualifiers of necessity and proportionality.

6.11. It can be observed that under Sections 8(6), 8(7) and 8(8) of DPDPB, which state that consent of a Data Principal will be "deemed" in certain situations which include cases such as for the maintenance of public order, purposes related to employment and in public interest, opening the door to wide & vague interpretation.

7. Privacy policy no longer required

7.1. Rule 4 of the 2011 Rules requires everybody corporate (or any person who on behalf of the body corporate) that collects, receives, possess, stores, deals or handles information of the information provider, to provide a privacy policy. Such a privacy policy has to be available for viewing by those who have provided any personal data to the body corporate under lawful contract(s). The privacy policy also has to be published on the website of the relevant body corporate. The privacy policy has to clearly set out the practices and policies of the body corporate for the collection, receipt, possession, storage, dealing or handling of information. It should also list out the types of personal data or sensitive personal data collected by the body corporate.

7.2. PDPB 2019 had gone a step ahead of the 2011 Rules and required that every data fiduciary should prepare a privacy by design policy, containing the following details:

(iv) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
(v) the obligations of data fiduciaries;
(vi) the technology used in the processing of personal data which has to be in accordance with commercially accepted or certified standards;
(vii) how the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;
(viii) the protection of privacy throughout processing from the point of collection to deletion of personal data;
(ix) the processing of personal data in a transparent manner; and

(x) the interest of the data principal is accounted for at every stage of processing of personal data.

7.3. Under PDPB 2019, every data fiduciary was expected to have its privacy by design policy certified by the data protection authority and published on the website of the data fiduciary and of the data protection authority.

7.4. Privacy policies have, over a period of time, become ubiquitous and almost all countries require them. DPDPB has dispensed with the need for data fiduciaries to put up a privacy policy on their websites. One can only hazard a guess as to why the Indian government has taken this approach, though PDPB 2019 had required data fiduciaries to post on their website a 'privacy by design' policy that has been approved by a regulator. It is possible that the Indian government feels that most data fiduciaries mechanically post on their websites data privacy policies, copied from somewhere else, without much application of the mind. Penalising those without a data privacy policy would not be an easy task, since there would be millions of cases of non-compliance. Ever since the 2011 Rules came into effect, there hasn't been any well-known instance of a data fiduciary having been penalized for not having put up a privacy policy on its website.

8. General obligations of Data Fiduciaries

8.1. DPDPB provides that notwithstanding any contract to the contrary or any omission by the Data Principal, Data Fiduciaries shall be primarily responsible for compliance with DPDPB and assume the following obligations:

(i) make reasonable efforts to maintain accuracy and completeness of the Personal Data processed when it is likely to be used for making decisions that affect the Data Principal, or it may be disclosed to another Data Fiduciary;
(ii) implement appropriate technical and organizational measures for compliance with DPDPB;
(iii) take reasonable security safeguards to protect Personal Data and prevent Personal Data breach, failing which could entail a penalty up to INR 250 Crore;
(iv) notify incidents of Personal Data breach[8] to the Board, as well as the affected Data Principal, failing which could entail a penalty up to INR 200 Crore;
(v) cease to retain Personal Data or remove the means to identity the Personal Data as soon as the purpose for its collection is completed and the data is no longer required for any legal or business purposes. It must be noted that DPDPB does not define 'business purposes', and the term can be used by Data Fiduciaries to retain data longer than required, negating the effectiveness of this obligation;
(vi) publish contact information of a grievance redressal officer who can answer the Data Principals' queries with respect to their Personal Data; and
(vii) effect mechanism for grievance redressal for Data Principals.

8.2. Pursuant to a contract and with the Data Principal's consent, DPDPB also enables a Data Fiduciary to engage a Data Processor[9] or transfer Personal Data to another fiduciary. Due care

[8] Personal data breach means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
[9] Data Processor is defined as any person who processes personal data on behalf of a Data Fiduciary.

must be observed here, as it may enable Data Fiduciaries to transmit Personal Data between their group entities which are also fiduciaries.

8.3. Overall these obligations of Data Fiduciaries are designed to ensure that Personal Data is processed in a manner that it respects individual privacy and data protection rights while allowing legitimate use of Personal Data for business purposes.

9. Significant Data Fiduciaries (SDF)

9.1. With a view to enforce a greater scrutiny of data processing practices, Section 11 of DPDPB enables the Central Government to classify a Data Fiduciary, or a class of Data Fiduciaries, as a SDF based on several factors such as the volume and sensitivity of the data processed by them, the risk of harm[10] to the Data Principal, potential impact on the sovereignty and integrity of India and other such factors mentioned under Section 11 of DPDPB. A SDF is required to carry out certain compliances mentioned under this Section in addition to the compliances mentioned under Section 9 which relates to compliances of the Data Fiduciary.

9.2. In addition to the obligations applicable to Data Fiduciaries, an SDF shall appoint (i) a data protection officer who is responsible to the SDF's board of directors or other similar governing body, and (ii) an independent data auditor to ensure that the SDF's is compliant with DPDPB. Lastly, an SDF is also required to conduct a 'Data Protection Impact Assessment' i.e., a process which assesses the harm with respect to processing of Personal Data and measures for managing risk of such harm.

9.3. Any SDF failing to comply with provisions of Section 11 may invite a penalty of up to INR 150 Crore.

9.4. The aim of the concept of SDF is to ensure that the entities which handle large volumes of Personal Data which is sensitive in nature are handled with high standards of data protection and are subject to additional regulatory oversight.

9.5. The following analyses specific aspects covered by DPDPB, namely (a) processing of personal data of children; (b) rights and duties of data principals; (c) cross border transfer and data localization; and (d) exemptions under the DPDP.

10. Processing of personal data of children

10.1. In their bid to recognize the criticism levied on the earlier drafts of the Bill, the legislature has attempted to include and provide adequate protection for children and their personal data under DPDPB. However, DPDPB fails to adequately include protections required to maintain the privacy of personal data of children, as intended.

10.2. To start with, the mere definition of a "child" under Section 2(3) of DPDPB itself has been worded to encompass children under 18 years within one sweeping definition. The legislature has thus failed to distinguish between teenagers, who have access to wider range of websites with a possible requirement to provide information and access data, from children (under 5

[10] The term "harm" encapsulates any bodily harm, distortion or theft of identity, harassment, prevention of lawful gain or causation of significant loss, each with respect to a Data Principal.

years, for instance) who need broad overarching protections and higher parental guidance and control.

10.3. This brings focus to the power given to parents and lawful guardians of the child, as defined under the definition of "data principal" under Section 2(9). DPDPB once again places a broad-based imposition on children's data by requiring "verifiable parental consent" in respect of all offline and online modes, which extends its reach to basic search-engines on any content. This severely restricts usage, almost amounting to surveillance, which restrict children's access to useful information, basic curiosity and knowledge-based learning as well.

10.4. Further, while DPDPB defines "consent" under Section 7, it is largely silent on the process of obtaining such consent from a data principal (including parents and legal guardian). One glaring issue is that usual verification is done by way of processing identities of individuals, which includes Aadhar card and personal information of such individuals. Therefore, under DPDPB, the verified consent required from data principals will probably include personal information of the data principal. Once again, by failing to specify the manner of seeking consent and the manner of verification of data principal by the data fiduciary, the procedure and information required for the same remains largely speculative if not problematic.

10.5. Interestingly, the definition of "harm" under Section 2(10) has been scaled down from the definition in the PDPB 2019, which could mean fewer protections. Although the PDPB 2019 did not have an exhaustive coverage of the meaning of "harm", it still covered issues such as humiliation, extortion, discrimination, and psychological manipulation, which are prevalent in the generation consumed by social media and behavioral/psychological games (reference to the Blue Whale suicide controversy). While the scaling-down of the definition may be looked at as an attempt to keep the definition broad enough for the Central Government to notify further meaning to it, the same once again grants arbitrary powers to the Central Government.

10.6. Meanwhile, the primary provision that concerns processing of personal data of children is covered in Section 10 of DPDPB, where obligations are aimed specifically for such data processing. However, apart from sweeping prohibitions against actions that may be "likely to cause harm to a child", such as, tracking, or behavioral monitoring of children, or targeted advertising directed at children, there are no specific nuances and issues tackled in the said provision.

10.7. Thus, DPDPB is largely lacking in its provisions concerning processing of children's personal data. Not only are the provisions aimed at restricting access rather than managing it, DPDPB skips protection of privacy of children and their data altogether.

11. Rights and Duties of Data Principals

11.1. DPDPB has included a whole chapter (Chapter 3) covering the rights and duties of data principals, with due recognition being attempted to be given to the right of a data principal over her personal data and her duty to not engage in actions such as, filing false and frivolous complaints, and suppress material information or impersonate another.

11.2. Data principals have been vested with rights to obtain information on their data being processed by the data fiduciary, including confirmation of it, status and summary of such processed data, identities of persons to whom such data has been shared with, and "*any other information*" as may be prescribed. DPDPB also attempts to grant greater control by data principal over their data by granting them the right to correct and erase personal data and the

right to grievance redressal (Section 13 and 14 respectively). Further, Section 15 grants the data principal, the right to nominate an individual in case of death or incapacity.

11.3. However, DPDPB fails in giving a completed look into protection of such rights by failing to detail procedures for data principals to seek information, or to file such requests for correction or erasure of their data, or appoint a nominee, or even register their grievance with the data fiduciary. Moreover, by doing away with damages or remedies in case of any such grievances or violation of rights of data principals, DPDPB is largely lacking in truly providing protection to the data principals over their personal data. Further, by leaving the power with the Central Government to "prescribe" the extent of information that may be protected from sharing DPDPB effectively gives authoritative and possibly arbitrary powers with the Central Government alone.

11.4. Meanwhile, DPDPB has included minimal duties on the data principals to ensure compliance with "all applicable laws" while exercising the rights under the provisions of DPDPB and prohibiting falsification of identity or filing false grievance or complaints. In continuation of the above discussion on data processing of children, this provision on duties of data principal could have explored the scope of duties that may have been imposed on parents and legal guardians acting as data principals on behalf of children. This could include provisions that would be restricting the extent of authoritarian control over the rights of data access by children, as per the requirements for access by the child as per their age group. However, DPDPB failed at capitalizing the opportunity to complete such all-rounded reforms.

12. Cross border transfer/ data localization

12.1. DPDPB surprisingly is largely muted on the issues concerning cross-border transfer/ data localization. While Section 4 provides that the Act shall apply to processing of digital personal data outside territory of India, if in connection with any profiling of, or activity of offering goods or services to Data principals within the territory of India, there are no provisions on procedures regarding the same. Meanwhile, Section 17 under Chapter 4, talks about transfer of personal data outside India. The provision however is a limited one, resting the power on the Central Government to notify such countries or territories, to which Data Fiduciary may transfer personal data, as considered necessary and as per such terms and conditions as may be specified. However, once again, there are no rules or regulations covering possible transgressions that may occur during such transfer of personal data. There are also no guidelines to be met by the Central Government, while considering notifying the names of such countries. As a result, there is concern over the ambiguity as well as the extent to which permissions may be granted in case of cross border transfer of data.

12.2. Albeit vague, the approach of MietY under DPDPB is largely concerning due factors including the bar that may be faced by data fiduciaries who may operate from countries that are not notified by the Central Government. This will prevent and restrict operations of such data fiduciaries who then shall not be permitted to transfer data necessary for running or processing their websites or provisions.

13. Exemptions under DPDPB

13.1. DPDPB provides for specific exemptions under Section 18, which covers two main aspects: the processing of personal data and the exemption afforded to Central Government.

13.2. Sub section (1) provides exemptions in case of processing personal data in the manner prescribed in Chapter 2 except those covering specific provisions (Section 9(4), Chapter 3, and Section 17. Such exemptions shall be allowed in case the processing is necessary for

enforcement of legal rights, or for performance of judicial or quasi-judicial function, or in the interest of prevention, detection, investigation or prosecution of offence or contravention of any law.

Meanwhile, sub-section (2) affords Central Government sweeping exemptions from the application of provisions of DPDPB, while processing personal data. This ensures far-reaching and arbitrary powers given to the Central Government to interfere, monitor, retain and collect data, and effectively breach or invade privacy of individuals, in stark breach of their right to privacy and security.

14. Enforcement Mechanism

14.1. DPDPB has a detailed compliance and enforcement framework for creation of the Board (as defined above) to be managed by a Chief Executive, appointed by the Central Government[11]. The Board will play the role of a regulator - having powers to pass directions/ orders[12], with the High Court being the statutory appellate authority[13]. The key features of the enforcement mechanism are as under:

(i) **Power akin to a regulator**: The Board has to perform the functions of determining non-compliances and impose penalties[14] and is to be guided by the principles of natural justice[15]. The Board further has power to direct the Data Fiduciary to adopt any urgent measures in cases where there is a breach of personal data, to mitigate harm or remedy personal data breach[16].

(ii) **Complaints/ Reference made to the Board**: Section 21 of DPDPB empowers the Board to take action based on (i) a complaint made to it by an affected person; (ii) reference made by the Central or State Government; (iii) directions of any court; or (iv) breach of duty by the Data Principal[17].

On receipt of a complaint, reference or directions as above, the Board has to first determine whether there are sufficient grounds to initiate an inquiry[18]. However, DPDPB does not define what are “sufficient grounds”.

Further, the Board has wide powers to summon and enforce attendance of persons, examine them on oath, inspect any data, book, document, register or books of account. The Board can also requisition services of Police officers, or any officer of the Central or State Government[19]. The Board has the power to pass interim orders pending an inquiry and its orders are enforceable akin to decrees made by civil courts[20]. The Board also has the power to review its own orders.

[11] Section 19, Digital Personal Data Protection Bill, 2022.
[12] Sections 20 and 21, Digital Personal Data Protection Bill, 2022.
[13] Section 22, Digital Personal Data Protection Bill, 2022.
[14] Section 20(1), Digital Personal Data Protection Bill, 2022.
[15] Section 20(2), Digital Personal Data Protection Bill, 2022.
[16] Section 20(3), Digital Personal Data Protection Bill, 2022.
[17] Section 21(2), Digital Personal Data Protection Bill, 2022.
[18] Section 21(4), Digital Personal Data Protection Bill, 2022.
[19] Section 21(9), Digital Personal Data Protection Bill, 2022.
[20] Section 22(13), Digital Personal Data Protection Bill, 2022.

However, the review must be carried on by a group larger than the one which held the proceedings[21].

(iii) **Excessive discretion with the Board**: Based on a determination as to a non-compliance being *significant* or *non-significant*[22], the Board may impose a financial penalty. DPDPB lays down no basis to come to the determination on what is a "significant" non-compliance and such a vacuum may give rise to the claim that the Board has broad and unfettered discretion.

(iv) **Provision of Voluntary Undertaking**: The Board has discretionary powers to accept voluntary undertaking with respect to matters related to non-compliance. On acceptance of voluntary undertaking, there shall be a bar on proceedings to the extent of the undertaking. Such a provision allows those who are non-compliant with DPDPB to avoid hefty penalties by curing non-compliance.

15. Penalty

15.1. The Board has been vested with the power to impose financial penalties on a Data Fiduciary, where there is (i) a non-compliance with DPDPB; and (ii) such non-compliance is *significant*. The quantum of penalty imposed has to be as per Schedule – 1, with a maximum penalty of up to Rs. 250 crores, which may subsequently be revised by the Central Government to up to Rs. 500 crores.

15.2. Further, DPDPB also lays down detailed parameters[23] based on which the Board shall determine the quantum of penalty, which include nature, gravity and duration of the non-compliance, type and nature of the personal data affected, repeat non-compliance, etc.

15.3. Interestingly, while DPDPB provides for a comprehensive framework for imposing penalties for non-compliances, there is no express provision for *compensation* to a Data Principal, in the event of negligence/ non-compliance by a Data Fiduciary. At the same time, DPDPB seeks to amend the Information Technology Act, 2000 ("**IT Act**") by omitting Section 43A which expressly allows an individual, whose sensitive personal data is misused, to seek compensation from an entity entrusted with data (akin to a Data Fiduciary). DPDPB does not contain a provision, similar to Section 43A of the IT Act, which empowers Data Principals to claim compensation before the Board. However, in our view, the current language of DPDPB, relating to powers of the Board, is broad enough to vest the Board with such power to grant compensation to an aggrieved person.

16. Rule Making Powers and Delegated Legislation

16.1. The Central Government is empowered to make rules from time to time, within the contours of DPDPB[24]. Each rule should be put before both houses of the Parliament for a total of 30 days, for ratification[25]. While not expressly stated in DPDPB, it appears that on expiry of 30 days

[21] Section 23(1), Digital Personal Data Protection Bill, 2022.
[22] Section 21(11), Digital Personal Data Protection Bill, 2022.
[23] Section 25(2), Digital Personal Data Protection Bill, 2022.
[24] Section 26(1), Digital Personal Data Protection Bill, 2022.
[25] Section 26(2), Digital Personal Data Protection Bill, 2022.

from the introduction of any proposed rules in either house of the Parliament, there would be a deemed ratification.

16.2. While the requirement for ratification of rules framed under DPDPB by the Parliament is a welcome step, there is a potential for abuse of the rule making power. Any rule introduced under DPDPB becomes effective immediately, even if it were to be later struck down by the Parliament. Nevertheless, all acts done under such rule, during the interim period, are deemed to be valid.

16.3. Pertinently, DPDPB seems to delegate many important aspects. Some important areas left to Central Government for rule-making are as follows:

(i) Situations which fall within the category of Deemed Consent[26].
(ii) Additional Obligations in relation to processing of personal data of children[27].
(iii) Additional Obligations of SDF to undertake Data Protection Impact Assessment[28].
(iv) Data Principal's Right to information about personal data from Data Fiduciary[29].
(v) Data Principal's right to correction and erasure of personal data[30].
(vi) Transfer of Personal data outside India[31].

Delegating important aspects of DPDPB might lead to legal challenges on the ground of excessive delegated legislation.

[26] Section 8(9), Digital Personal Data Protection Bill, 2022.
[27] Section 10, Digital Personal Data Protection Bill, 2022.
[28] Section 11(2)(b), Digital Personal Data Protection Bill, 2022.
[29] Section 12(4), Digital Personal Data Protection Bill, 2022.
[30] Section 13, Digital Personal Data Protection Bill, 2022.
[31] Section 17, Digital Personal Data Protection Bill, 2022.

Contributed by:

[Vinod Joseph, Partner]

[Udit Mendiratta, Partner]

[Jitendra Soni, Partner]

[Neha Madan, Partner]

[Shivkrit Rai, Associate]

[Shravya Karanth, Associate]

[Rohan Aneja, Associate]

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
knowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata
www.argus-p.com

MUMBAI
11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 6736 2222

DELHI
Express Building
9-10, Bahadurshah Zafar Marg
New Delhi 110002
T: +91 11 2370 1284/5/7

DELHI
155, ESC House, 2nd floor,
Okhla Industrial Estate, Phase 3,
New Delhi – 110020
T: +91 11 45062522

KOLKATA
Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

BENGALURU
68 Nandidurga Road
Jayamahal Extension
Bengaluru 560046
T: +91 80 46462300

www.argus-p.com I communications@argus-p.com