Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

**Date: 16th December 2022**

**To**
**The Ministry of Electronics and Information Technology**
**Government of India**
**New Delhi**

**Sub: Comments on the Draft Digital Personal Data Protection Bill 2022**

**Dear Sir**

Foundation of Data Protection Professionals in India (FDPPI) is pleased to share some of its thoughts on the proposed Data Protection Act in India based on the draft Digital Personal Data Protection Bill 2022 that has been released on November 18, 2022.

We shall be happy to provide any further clarifications that may be required on our suggestions.

**Yours sincerely**

**Na.Vijayashankar**
**Chairman**

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

| Chapter | Section | Suggestion | Reasoning |
|---|---|---|---|
| **I Preliminary (Preamble and Sections 1-4** | **Preamble**<br><br>**Suggested Modification** | WHEREAS the Right to Privacy is a fundamental right guaranteed under the Constitution of India subject to reasonable exceptions<br><br>WHEREAS with the increased digitization of the Society, Economy, and Governance, the need for protection of Information Privacy of individuals has become paramount,<br><br>WHEREAS the growth of the digital economy and advent of new technologies have rendered the current provisions of Information Technology Act 2000 inadequate to meet the Information Privacy protection requirements,<br><br>WHEREAS it is necessary to create a framework for Governance of personal data that ensures protection of information privacy of individuals in harmony with the duties of the Government and | In the light of multiple stake holders failing to arrive at consensus, the Data Protection law in India has remained on the drawing board for a long time. In this context, the approach of the Government to adopt a simple version of the Bill avoiding the contentious provisions is understandable.<br><br>However the "Dependency" on subordinate legislation itself can be a ground on which the Act could be challenged in Supreme Court and the Government should in anticipation make a few changes.<br><br>It is specifically felt that to weaken any prospect of legal challenge to the Act on the grounds of constitutionality, the Preamble may be strengthened appropriately. Our comments take this also into consideration.<br><br>The need for a law like DPDPB 2022 originated in the Supreme Court discussions on Aadhaar. This was followed by the Justice Srikrishna Committee report, following which other drafts on PDPB 2018/PDPB2019/DPA2021 originated.<br><br>The legislative intent that can be derived from these developments is that the law was required for "Protecting the Right to Privacy" of an individual. Though ITA 2000/8 and Section 43A as well as the accompanying rules were present even when Supreme Court sought and obtained an assurance from the Government that a "Privacy Protection Law" would be enacted, neither the Court nor the Government recognized the fact |

| | | | |
|---|---|---|---|
| | | requirements of Business, BE it enacted by Parliament in the Seventieth Year of the Republic of India as follows:— | that there was a law in India for protecting "Sensitive and non sensitive personal data" in the form of Section 43A and Section 72A of ITA 2000.<br><br>The Supreme Court in the Puttaswamy judgement stated that Privacy is a fundamental right but did not define the "Right to Privacy" in its judgement. The discussions in the individual parts of judgements in the Puttaswamy judgement by different Judges focussed on "Information Privacy" .<br><br>The Supreme Court in its Judgement did not clearly state that a law was required to be enacted for protecting the Right to Privacy per-se. They only discussed the need for protecting 'information' related to an individual. The Supreme Court presumed that in its reading of the Constitution, Privacy is already a fundamental right and there was no need for a law for this purpose though a procedural law was required for protecting "Information Privacy".<br><br>Hence Government coming up with a "Digital Personal Data Protection Act" is within the directions of the Puttaswamy Judgement. But this needs to be emphasised. |
| | **2(10)(a)**<br><br>**Suggested Modification** | Bodily or Mental injury | The definition of "Harm" is an important aspect of Privacy protection and hence over-simplification of the term is not considered advisable.<br><br>This definition will take care of the kind of misuse of data in Cambridge Analytica case or use of Dark Patterns or malicious manipulations such as the Blue Whale Game and Neuro Science related developments |

| | | | |
|---|---|---|---|
| | | | that adversely affect the autonomy of individuals and the sanctity of "Free Consent".<br><br>This extension is necessary to make the definition of "Harm" not limited to wrongful financial loss only. |
| | **2(10)(e) Suggested Addition** | Psychological or Neurological manipulation which impairs the autonomy of the individual; | **Same as above** |
| | **2(10)(f) Suggested Addition** | loss of reputation or humiliation or extortion | **Same as above** |
| | **2(10)(g) Suggested Addition** | such other harm as may be prescribed | **Same as above** |
| | **3(1)**<br><br>**Suggested Deletion** | **To be Deleted** | Section 3(1) states unless the context otherwise requires, a reference to "provisions of this Act" shall be read as **including a reference to Rules** made under this Act.<br><br>It is a standard practice in every legislation that rules will be notified to implement the broader provisions contained in the Act. |

| | | | |
|---|---|---|---|
| | | | It is not necessary to specifically make this statement and attract the attention of critics that the Act will be dependent on subordinate legislation. Section 26 takes care of this requirement. |
| | **Section 4(3)(d)**<br><br>**Suggested Deletion** | **To be Deleted** | It is noted that in Section 4 of the Act the subclause 3(d) states that the provisions of the Act shall apply to personal data about an individual that is contained in a record that is in existence for at least 100 years.<br><br>The purpose of this sub section is not clear. By 100 years, most individuals are dead and there is no reason why the right under this act should be extended to persons other than **living** natural persons.<br><br>This provision read along with the provision on amendment to Right to Information Act will be considered regressive and are not required in the Privacy Law.<br><br>Since as per our other suggestions, the personal information will be protected as long as a person is alive, held in trust for two years after death and later handed over to the Government, the rights of a deceased person's data becomes sovereign property after two years and the provision of 100 years is redundant.<br><br>**This has to be read with other suggestions related to Nomination.** |
| | **Section 4(3)(e)**<br><br>**Suggested Addition** | Personal data about an individual on an unauthorized stay in India | Though Privacy is a fundamental Right, it is subject to reasonable exceptions and such reasonable exceptions include national security. The Constitutional obligation is primarily directed to the citizens of the country and any extension to Non Residents is not to be considered |

| | | | |
|---|---|---|---|
| | **After the deletion of subsection (d) this section may be numbered as (d)** | | obligatory. Hence the law in its applicability can be restricted to "Citizens and Authorized Residents" in the country.<br><br>In view of the above, we suggest addition of subclause (e) to Section 3 as follows:<br>(This section will become 4(3)(d) if the suggestion to delete the current 4(3)(d) is accepted. |
| | **6(4) Suggested Addition** | The Data Fiduciary shall include in the notice information that represents an objective assessment of the compliance measures implemented and audited by an independent auditor. | Data Trust Score was one of the global firsts introduced in the earlier versions of PDPB which is presently absent from the current draft.<br><br>This should be available as a Compliance Maturity indicator and one of the desired compliance measures. For Large significant data fiduciaries above a threshold level of operation, publishing of DTS score should be made mandatory.<br><br>The Data Auditors may be provided an option to adopt their own system of DTS assessment which shall be mandatorily registered with the DPB. This will serve as the "Compliance By Design Policy".<br><br>Individual Data Auditors may be encouraged to adopt any Compliance By Design Policy with a DTS system registered with the Data Protection Board. |

| | | | |
|---|---|---|---|
| | **8(10) Suggested Addition** | Where identifiable personal data is meant to be used for direct monetization, consent shall be obtained only through Consent Managers.<br><br>The Consent manager shall be responsible to obtain an informed consent with appropriate safeguards.<br><br>The consent manager shall ensure that to the extent possible, anonymization, pseudonymisation or De-identification is used to secure the identity of the data principal and shall only let the identified personal data be used on a need to know basis depending on the type of processing involved for which the consent is obtained. | Innovation in technology need to be nurtured and law should provide channels where personal data may be used for business purposes provided the consent of the data principal is duly obtained and appropriate security measures are adopted.<br><br>Data including Personal Data is an industry raw material with which value is being created by technology. Every use of Data is ultimately leading to "Monetization" and hence there should be reasonable legal freedom to accept "Data Monetization" as a form of Data Processing which should be permitted as long as there are no harms to the data principal.<br><br>Anonymization and Pseudonymization or De-identification are known methods by which the identifiable personal data is securely processed without endangering the Privacy Rights of the Data Principal. Additionally law should provide a special provision where by under appropriate consent, Personal Data should be made available for "Monetization" in any form.<br><br>In order to achieve this progressive thought, In section 8, a new subsection (10) is suggested to be added with the following narration. This provision will bring an additional control in the form of the Consent Manager to prevent misuse of the consent. |
| | **8(11) Suggested Addition** | Where processing of identifiable personal data is carried out in a closed processing environment which includes anonymization and | Artificial Intelligence is being increasingly used in data processing and its use may be beneficial or harmful to the data principal. |

| | | | |
|---|---|---|---|
| | | or pseudonymization as part of the processing and the data output is devoid of identity, such processing is deemed to have the consent of the data principal.<br><br>The Data fiduciary shall have the obligation to ensure that the processing is programmed in such a way and supported with reasonable assurance that no human including the admin of the system has visibility of the identity parameters associated with the personal data. | Information Technology Act 2000 clearly identifies that actions of an automated system are attributed to the person who caused the system to act in the manner it so acted. Hence the actions of Artificial Intelligence algorithms are attributed to the owner of the AI algorithm who in turn needs to obtain assurances from the developer/seller of the AI algorithm.<br><br>Since this aspect is not clear in the data protection scenario, there is a need to clarify the role of AI algorithms whether it is to be considered as a "Data Processing" without a human interference and how the attribution aspect mentioned in ITA 2000 becomes applicable.<br><br>Further many processes in personal data processing happens within a closed system and the human users of the system including the admin may not have visibility to the identity attached to the processed personal data. Also the output may be devoid of any identity.<br><br>Such processing may be considered as "Combo Processing" where the key element of processing which could be aggregation, filtering, pruning, tuning etc is combined with the security processing of anonymization or pseudonymization . Like processing in a homomorphic encryption situation, the privacy aspect of the data is not tampered with during such processing. Such processing needs to be encouraged and incentivised.<br><br>The above aspect can be reflected in the draft under the "Deemed Consent" provision by adding an additional sub clause as follows. |

| | | | |
|---|---|---|---|
| | **8(12)**<br><br>**Suggested Addition** | Where a valid consent has been obtained in the case of a Data Principal who is a minor or otherwise incapacitated, such consent will continued to be valid upto a period of 3 months after the incapacitation is removed or the person attains majority or until a valid new consent is provided by the erstwhile incapacitated person. | One of the issues that a compliance nightmare is the transition of a minor's data from parental consent to self consent at the time of his attaining majority. At the stroke of midnight when a person turns 18, the parental consent for processing of the data becomes infructuous. Ideally in such a situation, the processing must be stopped until a consent is provided by the erstwhile minor who is presently a major.<br><br>In order to provide business continuity, it is necessary to provide for a reasonable transition time for such cases.<br><br>We therefore suggest that the processing of the minor's personal data under a valid parental consent may be continued for a period of about three months after the person attains majority or until a new consent is provided by the now major data principal.<br><br>For this purpose the erstwhile consent may be considered as a "Deemed Consent" of the data principal for a period of 3 months after the data principal attains majority. |
| | **Section 9(10) Suggested Addition** | In the event of the receipt of a notice of death of a data principal, the Data Fiduciary shall consider the consent provided as terminated and shall take such reasonable steps as required to inform the legal heirs of the deceased to take necessary steps to claim residual | This is to make the Data Fiduciary responsible for ensuring that the legal heirs of the deceased data principal are suitably informed to exercise their rights through appropriate means like settlement of a claim in a Bank. |

| | | | |
|---|---|---|---|
| | | rights if any on the data which had been placed in the hands of the data fiduciary by the data principal.<br><br>In case no claimants can be located, the information shall be held secure for a period of 2 years after which the data shall be deposited and archived with the Data Protection Board or such other suitable authority of the Government of India designated for the purpose. | This has to be read with the reasoning provided for modification of Section 15<br><br>The above suggestion presumes that "Data has a value" and may consist of pointers to digital assets such as **"E-Rupee"** and hence is to be considered as a "Sovereign Asset" if unclaimed.<br><br>This may require the DPB to set up a "Data Vault" and designate a custodian to manage the data as a sovereign asset. This will have to be added under the functions of the DPB as under. |
| | **9(11) Suggested Addition** | The Data Protection Board may specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act in consultation with the sectoral regulators and representatives of the industry and the data principals. | The entire compliance requirements of a Data Fiduciary have been concisely presented in the Act under Chapter II.<br><br>In PDPB 2019, under Section 50 there was provision for the industry to establish acceptable codes of practice which could be approved by the authority and adopted. This was a "Self Regulatory System" with wide implications on sectoral regulations.<br><br>In the current draft this provision has not been specifically indicated and it is presumed that the principle will be introduced through the Notification.<br><br>While providing such notification, it should be ensured that India should encourage indigenous frameworks of compliance by introducing the provision for "Approved Code of Practice". |

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

| | | | |
|---|---|---|---|
| | **11(2)**<br><br>**Suggested Addition** | Explanation:<br>The Data Protection Officer shall be based in India and may include a consultant who is not an employee of the Data Fiduciary.<br><br>The Data Auditor shall be based in India and shall be an independent person and shall not be an employee of the data fiduciary.<br><br>All contractual data protection officers and data auditors shall be registered with the Data Protection Board as may be prescribed. | **This has to be read with the detailed reasoning given below for 11(2)(d)** |
| **II Obligations Sections 5-11** | **11(2)(d)**<br><br>**Suggested Addition** | Large Significant data fiduciaries with a turnover of over Rs 50 lakhs per annum shall register themselves with the Data Protection Board as prescribed along with particulars of the Data Protection Officer and his contact details.<br><br>Explanation: The Data Protection Officer shall be based in India and may include a consultant who is not an employee of the Data Fiduciary. | Large Significant data fiduciaries with a turnover of over Rs 50 lakhs per annum shall register themselves with the Data Protection Board as prescribed along with particulars of the Data Protection Officer and his contact details. |

| | | | |
|---|---|---|---|
| | | The Data Auditor shall be based in India and shall be an independent person and shall not be an employee of the data fiduciary.<br><br>All contractual data protection officers and data auditors shall be registered with the Data Protection Board as may be prescribed | |
| **III Rights Sections 12-16** | **13 Suggested Addition** | **Explanation:** Right to "Erasure" under this section does not include the "Right to Forget" which shall be subject to an appropriate order of the Data Protection Board. | In the PDPB 2019, "Right to Erasure" and "Right to Forget" were treated as two different rights and "Right to Forget" was kept as the discretion of the adjudicator.<br><br>In the current version, this distinction is not clear and there will be confusion about whether Section 13 includes "Right to Forget". In the Indian context where the threat of terrorism is very high, leaving the "Right to Forget" as a general right to be exercised by a Data Fiduciary at the request of the data principal is not safe. This will provide an opportunity for criminals to cover their tracks before a crime is discovered and will also conflict with several provisions of Information Technology Act.<br><br>Hence "Erasure" should be limited to removal of the information from the active processing space and not extended to complete removal of the identity from the records of the data fiduciary. |

| | | | |
|---|---|---|---|
| | | | Even in the few Court decisions on Right to Forget, only public disclosure has been masked as part of the right to forget and not complete removal.<br><br>Further, "Right to Forget" is an over reach of "Privacy" introduced by the EU and is actually an alteration of a historical fact. It interferes with the "Right to Information" of the public and does not need to be kept hidden.<br><br>Allowing a historical fact hidden is a crime against the society and law should avoid promoting this trend. |
| | **Section 14(1)**<br><br>**Suggested Modification** | A Data Principal shall have the right to readily available means of registering a grievance with a Data Fiduciary including for claiming compensation for any loss or damage suffered by him on account of non fulfilment of the obligations under this Act by a Data Fiduciary. | Further, the prescribed Penalty system or the Rights do not mention the Right of a Data Principal to claim compensation. This would be the biggest weakness of the Bill to prove that it is not "People oriented" and will be used as an evidence of the Bill ignoring the mandate of the Supreme Court that an individual's privacy is a Right to be protected.<br><br>If left as it is, individuals have to invoke ITA 2000 and claim compensation under Section 43 whenever a data breach occurs. This will bring in the Adjudicator under ITA 2000 as another regulatory authority into the Digital Data Protection Regime.<br><br>Lack of the Right to claim compensation would be considered as a serious lacuna in the law in the global evaluation and without such provision, other laws will not consider the provisions "Adequate". |

| | | | |
|---|---|---|---|
| | | | Hence it would be most essential to provide the "Right to compensation" either in the Chapter III (Rights) or under Penalty.<br><br>This can perhaps be also added in the Section 14 of the draft under "Grievance Redressal" by modifying Section 14(1) as follows.<br><br>PS: This insertion of Right to be compensated against "harm" will essentially guarantee the Right to Privacy in operational terms linked to the definition of harm. Once included in the grievance, it also comes within the purview of the Data Protection Board during adjudication and goes into the legal system of High Court and the Supreme Court. |
| | **15**<br><br>**Suggested Modification** | Subject to other laws in force, a Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the **event of death or incapacity** of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act.<br><br>For the purpose of this section, "incapacity" means inability to exercise the rights of the Data Principal under the provisions of | Section 15 of the draft recognizes the "Right to Nominate" an individual to "Exercise the rights of the Data Principal" in the event of death or incapacity of the Data Principal.<br><br>This provision provides a deemed recognition to "Data" as a "Transferable Property" . "Data" however is more appropriately not a "Property" but is a "Special legal right" more akin to the intellectual property right that can be assigned during the life time of the owner as is envisaged under the "Consent Manager" scheme.<br><br>"Consent" is in the nature of a "Contract" which also is operable only during the lifetime of the individual as per the Contract Act. |

| | | | |
|---|---|---|---|
| | | this Act due to unsoundness of mind or body. | The provision also does not recognize the limitation imposed by Section 1(4) of the Information Technology Act which does not legally recognize a document in electronic form which is in the form of a "Will" or any transfer of right that will occur on the event of death of a person. It is ultra-vires ITA 2000 at present.<br><br>Further even in the case of "Incapacitated" persons, nomination will be a right that the person himself cannot exercise after incapacitation. If allowed, this provision is subject to misuse and abuse in the case of a vulnerable data principal during his life time.<br><br>Hence Section 15 appears to pose some legal conflicts that needs to be addressed.<br><br>As regards the exercising of rights related to a person who is incapacitated either because he is a minor or mentally or physically in a state where he cannot exercise a logical decision, while the person is alive, the law of contract may provide a solution.<br><br>However, without ITA 2000 being amended, the "Nomination" facility on the death of a person poses a legal problem.<br><br>Due to security and Cyber Crime considerations, it is not advisable to remove the provision under ITA 2000 which prohibits a "Will" in electronic form. But ITA 2000 does not prohibit a "Will" in respect of a digital property executed in written form. This needs to be retained even under this Act for nomination. |

| | | | |
|---|---|---|---|
| | | | (However the consent in cases of persons without contractual capacity should be a special consent with witness like the contracts executed by illiterate or blind persons.)<br><br>If Section 15 states "Subject to the provisions of other applicable laws…." then it would mean that nomination has to be done through a non digital document where necessary. |
| **IV Special Provisions Sections 17-18** | **20(5) Suggested Addition** | The Board may set up a Data Vault to archive unclaimed and abandoned data with Data Fiduciaries and designate a Custodian to dispose of claims on such data, transfer the realisable value if any to the consolidated fund of India and eventually destroy the data under controlled environment. | This has relation to the suggestions regarding Nomination under Section 15 and also the obligations under 9(10) |
| **V Compliance Framework Sections 19-25** | **25(1)<br><br>Suggested Modification** | If the Board determines on conclusion of an inquiry that noncompliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose such financial penalty as specified in Schedule 1, not exceeding rupees five hundred crores or 2% of the total worldwide turnover. | It is noted that the Government has taken a policy decision to use absolute figures to depict the maximum penalty provided under the Act instead of representing it as Percentages of turnover.<br><br>However in the process, the maximum penalty has been pegged at Rs 500 crores per instance where as, in the World of GDPR, GDPR penalties have been imposed over Rs 6000 crores at present. Hence Indian law appears extremely conservative. |

| | | | |
|---|---|---|---|
| | | **Explanation:** the expression "total worldwide turnover" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India. | While the change could be welcome for the Big Tech Companies, SMEs may feel that they may be subjected to crippling penalties since in their case the penalties at the maximum level of Rs 500 crores may be disproportionately high compared to their turnover or profits.<br><br>While we can always justify that the DPB (Data Protection Board) would exercise discretion in case of SMEs taking into account their ability to pay as per Section 25(g) of the draft Bill, the same discretion could have been relied upon by depicting the penalty in terms of percentages.<br><br>The percentage-based penalty has been an accepted norm now in Data Protection Laws. It may be noted that in certain countries have based the penalties on the local country turnover but hiked the percentage upto 10. Hence it would be in order to retain the percentage based penalty structure as in the previous draft.<br><br>If there is an argument that uncertainty in defining "Global/total worldwide Turnover", we may say that similar uncertainty remains in interpreting "Each Instance" as used in the Act.<br><br>An instance can be a "type of vulnerability" exploited (as in HIPAA) or a set of breaches that have occurred "at a point of time". Normally a breach consists of thousands of instances spread over a period and it is possible that we may technically consider each breach as an instance. The breach would also consist of multiple types of failures |

| | | | |
|---|---|---|---|
| | | | both technical or organizational. Hence defining an "Instance" is as much complicated as defining "Global" in terms of turnover.<br><br>We also observe that under HIPAA-HITECH Act, USA which uses a similar penalty system based on "Maximum penalty per type of Contravention", has even used an inflationary adjustment on the maximum penalty prescribed in fixed terms. This is an innovative method to ensure that like in IPC, law does not get stuck with a fine that ceases to be a deterrent because the value of Rupee is different from what it was when the law was enacted. |
| **VI Miscellaneous Sections 26-30** | **30(2)**<br><br>**Suggested Deletion** | To Be deleted | Section 30(2) seeks to amend the Right to Information Act which protects "Privacy" over and above the "Right to Information".<br><br>This is in conflict with the national security posture of the other aspects of the Bill and opens up a needless controversy.<br><br>The current Right to Information Act provides protection of privacy within its current provisions as a decision to be taken by the information officer and this should be considered sufficient to protect the Right of Privacy. |