Naavi.org

Building Cyber Jurisprudence for a Responsible Cyber Society in India...Since 1998

No 37, Ujvala, 20th Main, BSK First Stage, Bangalore 560050: www.naavi.org: naavi@naavi.org: +919343554943

Draft Comments on DPDPA Rules 2025

Comments

Rule No	Comments
1	a) It is recommended that the notification prescribe that DPB shall be formed within 3 months and commence its operational website within 4 months of the notification. b) Provisions related to Registration of Consent Manager may commence once the DPB becomes operational. c) Compliance requirements such as Consent, Data Breach Notification and Restrictions on transfer of data outside India (Where applicable) may be notified as required before 6 months from the commencement of DPB and d) Penalties under Section 33 may be notified as becoming effective effective after one year. (DPB may use its discretion to use the provision of voluntary undertaking to grant time where it is considered necessary). e) Section 44 DPDPA 2023 should be specially mentioned as becoming effective along with Section 33 so that Section 43A of ITA 2000 (Information Technology Act-2000) will be replaced only after the penalty clauses under DPDPA 2023 becomes effective. f) Provisions of 10(2)(a) [DPO] may be made effective within 6 months g) All other residual requirements under the Act may be notified as applicable at the end of one year from notification.
2	**Definitions:** No Comments.
3	**Notice to be given to the Data Principal:** **Legacy Data Principals** A mention may be made that notice in the same format is required to be sent to all legacy data principals. a) Where the Data Fiduciary does not possess valid email or SMS contact information, it may be prescribed that a notice shall be published through advertisements in one English and one Prominent local language newspaper. b) A web notice shall also be published on the data fiduciary's website which shall be searchable by Search Engine robots so that data principals may pick up the notice through their web searches. c) It is necessary to also indicate that where no valid response is received from the legacy data principal within a reasonable time to continue processing, all instances of the data in the custody of the data fiduciary including in back up storage shall be deleted.

	d) The time to deletion may be prescribed as 3 months and after 2 monthly reminders followed by a 48 hour notice to deletion. As a precaution against future disputes, the "Legacy Data Purged under this rule by the data fiduciary" may be archived under a **"National Personal Data Archive"** to be created by the Government with suitable security and retrieval capabilities. The archive may have two parts one of which may be **"Unclaimed Data"** and the other "**Archived for legal necessities**". While the "Unclaimed Data" would contain all data where consents could not be obtained or nominees not appointed or nominees cannot be identified, the second part may contain data that needs to be retained for long or indefinite period either because they are evidences in a legal dispute or required under some other law. The creation of "National Personal Data Archive" will ensure that the sovereign data of Indians shall be preserved for whatever it is worth in future and its value for the history of the nation.
4	**Consent Manager** **Part A of the First Schedule provide information on the requirements to be fulfilled for registration of a Consent Manager.** a) The rules prescribe that the Consent Manager shall not have the visibility of the data. At the same time it is also prescribed that the Consent Manager shall have a minimum net worth of Rs 2 crores, does not use the services of a data processor, follow several restrictions and disclosures to prevent conflict etc. This is self contradictory for the reason that if the Consent manager has no visibility on the data exchange and needs to only maintain the personal data to the extent of maintaining the account of a data principal which is a low sensitivity personal information , the reason for stringent "Fit and Proper" criteria is not clear. On the other hand these restrictions and disclosures are relevant if the Consent Manager has access and visibility to the personal data of an individual which is being exchanged. In such a case the criteria that the Consent Manager shall be a company constituted in India needs to be supplemented with the condition that the share holding shall be held in majority by Resident Indians. In the event the Consent Manager is only having visibility to name, email address and mobile number of the data principal and no other information, there is no need for all the restrictions and disclosures and they may be removed. On the other hand if the disclosures and restrictions are intended with a purpose, it is presumed that in future the Consent Manager may be permitted to have access to the personal data exchanged in the encrypted channel from the data fiduciary in possession of the required data and the data fiduciary in need of the data or the Government is expressing a lack of confidence that the Consent Manager may pry into the confidential data exchange. This needs to be clarified. b) Since the personal data is not visible, the "Consent" retained by the Consent Manager for 7 years irrespective of the actual period for which the data is likely to be in use with the data fiduciary user, the record will only show the log record of the transaction without the information there in. For example, the Consent Manager knows that X data fiduciary requested a Bank account number from Y data fiduciary and after obtaining the consent of the data principal, the consent manager facilitated the flow of the encrypted data from Y to

	X in an encrypted channel. However the Consent Manager does not know what was the account number. If this data is later deleted by X (and perhaps Y also), the need to retain the transaction data for 7 years by the Consent Manager seems not logical. It can be removed or limited to the period upto which the Data Fiduciary user (X) retains the data related to the consent. c) A reference has been made to "Digi Locker" as an example of a service that can act as a "Consent Manager. However, since the Digi Locker is a "Document Repository" and not a "Data Repository", the example is not appropriate. Hence reference to Digi Locker seems not relevant. The reference to Digi Locker may therefore be removed. Since the purpose of the Consent Manager is only related to keeping record of consent sought and consent given, and this requires the consent of the data principal each time, in a given practical situation, The data principal will be stalled at the data fiduciary user site waiting for the consent to be delivered from the Consent Manager adding delay and information overhead to the system Hence there is a case for the suggested system to be changed in one of the following two ways i) Remove most of the restrictions and disclosures in view of the Consent Manager not handling any sensitive personal information of the data principal ii) Retain all the restrictions and disclosures but provide visibility to the personal data of the data principal
6	**Processing by State** It may be clarified how consent may be obtained in case "Previous Consent" is not available or when the "Reference of previous consent" is not traceable. Since there may be cases where subsidy or payments may be paid regularly to "Non-Existent" persons, it is beneficial to eliminate such fraudulent payments by stating that "In cases where the existence of previous consent may not be traced nor a new consent is available, the processing shall be stopped and the payment of subsidy etc discontinued".
7	**Personal Data Breach** This rule refers to intimation of personal data breach. The Rule prescribes a two-stage reporting one to be made immediately on being aware of the personal data breach and the other within 72 hours with more details. It is necessary to recognize that there are cases of false alarms and incidents which may be whistle blowing reports which if confirmed may become breaches but could turn out to be false. Hence the report to be submitted "Forthwith" should be termed as "Provisional". The confirmed report filed within 72 hours may be called "Personal Data Breach Report". Further some "Personal Data Breaches" recognized as such as per the definition under DPDPA 2023 may involve infringement of Data Principal Rights and not exfiltration or "Loss" of personal data from the custody of the data fiduciary. These are not as harmful as the data breaches involving exfiltration of data or modification of data. This has to be factored in to the definition of "Personal Data Breach". Hence there is a need to recognize three categories of personal data breaches namely a) Provisional Data Breach b) Data Breach not resulting in loss of data c) Data Breaches resulting in loss of data The rules should treat these differently.

	It is necessary to recognize that every personal data breach involving loss or damage to data is also a data breach under ITA 2000 and is reportable under CERT IN guidelines even after the repealing of Section 43A. Hence clarity should be brought in about need to copy the provisional and the final data breach report to CERT IN. The personal data breach not involving loss of data need not be reported to CERT IN. However, such data breach may also be a part of the possible claim of damage by the data principal under adjudication proceedings of ITA 2000. There should be a process where the DPB and CERT IN act in harmony dealing with the breach report. Since CERT IN has an infrastructure to provide technical guidance of remediation, there is no need to duplicate the efforts at DPB. Regulatory investigation of technical nature if required should be left to CERT IN and adopted by DPB. For this purpose, a "DPB-CERT IN Data Breach investigation policy" should be announced which may specify a time bound completion. Alternatively, changes should be notified under ITA 2000 stating CERT IN would refrain from investigating such cases which are taken up for investigation by the DPB under DPDPA 2023. This would however require additional technical investigation capabilities to be built up by DPB. On the other hand, CERT In has the necessary expertise and a team of scientists who can have access the CERT IN auditors and this infrastructure needs to be utilized. There is a need to recognize that DPB would be more interested in identifying noncompliance of law which may affect the rights of the data principal and hence would like to track even such personal data breaches which do not result in exfiltration of data that causes irreversible damage to the data principal. On the other hand, CERT IN is more interested in prevention of Cyber Crimes and hence focussed on data breaches involving exfiltration of personal data. Hence there is a need for a re-look at this rule and a simultaneous change in the CERT IN rules related to data breach.
8	**Erasure of Personal Data** The rules should distinguish the terms "Deletion" and "Archival" in the definition clause itself and include data which has completed its purpose but is required to be held till expiry of the period mentioned or when it is to be retained for other legitimate purposes should be "Securely archived". It is also suggested that the Government of India should set up a "National Archival of Personal Data" and like Banks transferring unclaimed money into a separate account, should transfer the unclaimed personal data into this archive. This will relieve the burden of holding personal data that is not used for active processing within the custody of the data fiduciary. Such "Unclaimed" personal data may also arise because of the death of the data principal which the data fiduciary may not be aware of. Schedule III provides that the data retention up to three years applies to certain types of data fiduciaries and having more than stated number of registered users in India. Clarity should be provided regarding other types of data fiduciaries and those having less than the prescribed number of subscribers in India. (2 crores or 50 lakhs as the case may be) It is recommended that the 2 crore subscriber limit may be deleted and the need for "Deletion" converted into "Porting to the National Personal Data Archive" The definition rule should therefore add definition of "Archival", "National Archival of Personal Data".
9	**Business Contact** This rule recognizes the term "Business Contact" which is not otherwise defined. An explanation may be added that "Information in the nature of Name, E Mail or Phone number provided by an individual to another entity for business purpose shall be deemed as Business Contact and as Non-Personal Data. .

10	**Verifiable Consent for Minors** Before processing personal data of Children, the Act prescribes that a "verifiable Consent" of the guardian is obtained in such a manner as prescribed. The rules prescribe that the data fiduciary shall observe "Due Diligence" to confirm that the person identifying himself as the "parent" should be verified if he is not a minor himself and goes on to say the identification is required in the interest of prevention of any offence etc. The fact that there is a need to first identify that the data principal himself is a minor is more challenging since this is required for every data principal. This must be part of the first stage of verification and should be part of every notice and consent. Without this verification, any minor can declare himself not to be a minor and avail services including purchase of drugs and prohibited goods on e-commerce websites. It is only when a data principal declares that he is a minor that he may refer to another person as his guardian (may be better word than patent) who must then identify himself that he is not a minor and he is the parent or otherwise a legally appointed guardian (both for minors and in the case of disabled persons). A reliable reference to the identity of a person as the parent and the age of the minor is available in the Aadhaar data and it is the only means of reliable verification. Using "Virtual Aadhaar" and a "Yes or No" query would meet any objections of Anti-Aadhaar lobby and can be defended even in a Court. MeitY should encourage development of a specialized "Consent Manager for Minors" who can handle this responsibility of "age-gate management and parent identification" with reference to the name of the parent in the Aadhaar card of the minor. Ministry specify that "Yes-No query" for "Name of the principal", "Age" and "Name of Parent if any" should be made mandatory for all services. This will also address the "Fake Identity" in social media. This can be effectively implemented by the Consent Managers and encourage Data Fiduciaries to use the services of Consent Managers. MeitY should encourage UIDAI to issue a "Age Card" for all Aadhaar holders so that without disclosing the other Aadhaar information, the age alone can be verified by third parties. In case of Minors, the name of the parent should be included in the "Age Card" MeitY should also encourage Chief Justice of India to suggest that in all cases where the Court appoints a legal guardian both for Minors or Disabled persons, the Court should direct UIDAI to issue a Card that designates the disabled person and the designated guardian. UIDAI may provide support to some specialized Consent Managers who are authorized for this purpose as Authorized User Agency and a Consent Manager under DPDPA 2023.
11	**Minor-Behavioural Tracking** This rule refers to the prohibition of tracking or behavioural monitoring of minors or disabled persons. The fourth schedule specifies that certain data fiduciaries for certain functions are exempted from this provision. The exemptions provided to educational institutions is limited to the protection of health and safety of the children as well as Creches, Childcare centres and child transport services. However, the educational institution itself is not exempted in terms of tracking of the educational progress of the child. This needs to be added. .

12	**Significant Data Fiduciary** This rule relates to Significant data fiduciary (SDF) and his obligations. The Act specifies that the Data Protection Officer (DPO) "represents" the SDF under the provisions of the Act. The Rule however only specifies that the DPO shall be the "Point of Contact" for "answering" the questions raised by the data principal. The rule should at least say that the DPO shall be the point of contact for "resolving" the questions raised. The Rule states that the SDF "In addition to the measures provided under the act" undertake the periodic Data protection Impact Assessment (DPIA) and the periodic audit under the provisions of the Act at least once in every year. The "DPIA" and "Periodic audit" are mentioned as two different aspects, and both are indicated as required once a year reckoned from the date when the rules come into force, or such data fiduciary becomes an SDF whichever is later. While it is understandable that the "Periodic Audit" as per section 10(2)(b) is indicated as an annual audit, the DPIA by concept should have been indicated as to be conducted as and when a new process for processing personal data is introduced which gives rise to a new risk. Further, it would be better if the provision that the DPO should be "Based in India" is further clarified as to what is the meaning of being "Based in India". It should be clarified such as to mean, that the salaries are paid out of India or residence in India should be more than 6 months in a year etc. The Act is interpreted to mean that the DPO should be an employee and the Data Auditor should be an external independent person. This may be clarified along with an exemption for SME/MSMEs or companies with a turnover less than say Rs 1 crore per annum, that they can appoint a compliance manager within and take the assistance of a DPO from outside in case necessary. Further the expected credentials of the DPO and Data Auditor could be indicated at least in broad terms. It is welcome that MeitY may designate an official to clarify on who is a Significant Data fiduciary and who is not. In this connection, it may be suggested that the limit of subscribers to determine the threshold of an SDF could be related to the sensitivity of the data processed. For example, if "Health" and "Finance Data" are considered sensitive, the limit may be considered as around 50000 or less. On the other hand, for more sensitive information such as Biometric the limit can be around 10000 or less. For information such as DNA the volume limit may be eliminated. For mere demographic or contact information such as the social media intermediaries, higher volumes such as 50 lakhs used in ITA 2000 may be retained. Hospitals or Banks may be declared as SDF irrespective of their size. Individual DFs subject to their type of activity such as handling large quantity of minor data or handling defence supplies etc may be declared as SDFs individually. Also, every Data Processor of a Data Fiduciary who determines the "Means of Processing" by themselves including the Black Box implementation of AI algorithms must be considered as a Data Fiduciary jointly with the Principal Data Fiduciary and if the principal data fiduciary is a Significant Data Fiduciary, the Joint Data Fiduciary also must be considered as a Significant Data Fiduciary. It is necessary that DFs should be provided a facility to enquire and register themselves as SDF through some published criteria which can be validated by the DPB on application.

	It should be mandated that every DF should voluntarily file an application for being considered as "Provisional SDF" or being exempted from being considered as "SDF" through the website of the DPB. At that time, the DF may be required to file a DPIA to substantiate its application. The responsibility to declare themselves as "Provisional SDF" must be put on the DFs since it would not be feasible for DPB to identify those DFs who fail to recognize themselves as SDF and implement the special obligations envisaged. It is also suggested that the categorization of SDF can be process dependent so that the same organization may declare different processes some of which are SDF processes, some data Processing for other DFs and some its own DF processing. An organization can be considered as a hybrid entity of DF, SDF and contractual data processing operations and compliance requirements can be applied differently if the activities are properly segregated, and arm's length relationship is maintained between the processes like the "Hybrid entity concept of HIPAA". The process-based compliance is essential since the collection of personal data is also process dependent and data minimization, data retention minimization and purpose definitions may all be linked to a process rather than the entity. Considering the many doubts that the implementers of the Act may face a provision for making a "Prior Reference" of the "Compliance Framework" to DPB may be introduced on the lines like the registration of "Privacy by Design Policy" envisaged in the previous version of the data protection law. (PDPB 2019).
13	**Rights of Data Principal** This Rule refers to the Rights of the Data Principal and measures to be initiated by a DF for protection of the rights. The rule provides that the DFs may indicate their own means of identification of a data principal for granting any of the rights including exercise of nomination rights. The means of identification in case of legacy data for which the previous consent may be inadequate in identifying the data principal is a challenge for DFs and the rules could have provided appropriate guidelines. In the absence of say the e-mail address or mobile number, or a total absence of consent document for reference, the possibility of providing any information at the request of a person claiming to be a data principal is a security risk. In such cases, it is recommended that the rules provide that the data principal may be mandated to provide a KYC verification at his cost. This would be another incentive for encouraging users to opt to go to Consent Manager services. In case of request for correction and withdrawal of consent if the data fiduciary does not agree with the data principal the matter will be a subject matter of dispute to be settled by the DPB. There may be some instances where the request for deletion cannot be accepted without the risk of violating other laws such as Information Technology Act 2000. In such cases the disputed data may be archived securely outside the custody of the Data fiduciary. For this purpose, it is suggested that the Government may set up a Personal Data Repository/National Archival of Personal data and store the data under their control. Required provisions may be made in this regard in the rules. Considering the legal hurdles on getting an electronic instruction of a data principal after his death in view of Section 1(4) of Information Technology Act 2000, a complete code for handling registration of "Nomination" and settlement of claims should be developed.

	There is a need to define "Nomination of Personal Data" and means of transferring the safe custody of personal data on receipt of confirmed information of the death of a data principal. Since the responsibilities of settling the claims are onerous, the possibility of porting the data to the Government repository may be considered as one of the options for settlement of claims. The Personal Data Claim settlement for deceased Data Principals can be an agency of the Government which can work with the National Archival of Personal Data. Necessary provisions may be made under the rules for this purpose. Under the suggested process the personal data of the deceased data principal may be securely handed over to the Custodian under the scheme who may handle the claims instead of the Data Fiduciary.
14	**Processing of Personal data outside India** The provision to retain the possibility of introducing restrictions on persona data transfer to other countries is welcome.
15	**Research and Statistical Purpose** There are no specific comments.
16	**DPB Constitution** There are no specific comments.
17	**Salaries and Allowances of Chairman and Members** There are no comments.
18	**Proceedings of DPB** There are no comments
19	**Functioning of the Board as a Digital Office** This rule suggests the use of digital means of conducting the affairs of the DPB. It is welcome.
20	**Service terms for officers** There are no comments
21	**Appeal to TDSAT** This Rule indicates the procedure for filing an appeal by a person aggrieved by the decision of the Board to the Appellate Tribunal which is the TDSAT. The procedure is determined more by TDSAT itself and MeitY may not have any powers to suggest the procedure for handling the appeal. Hence this rule needs to only indicate that the procedure for DPB to permit appeal to TDSAT and leave the rest of the procedures to TDSAT.
22	**Calling for information from Data Fiduciary or Intermediary** This rule provides through the seventh schedule that the Government may designate specific officials for purposes such as notifying the significant data fiduciaries or for declaring certain exemptions. This may be the only provision that has been invoked under the residual powers of rule making under Section 40(z) There are no comments