Foundation of Data Protection Professionals in India
(Section 8 Company, Not for Profit, Limited by Guarantees)
CIN Number: U72501KA2018NPL116325:
GSTN: 29AADCF4963H1ZC
www.fdppi.in: E Mail: fdppi@fdppi.in : Ph: 8310314516

Comments on the Draft Rules released for selective discussion

To

The Secretary
MeitY
New Delhi

Dear Sir

As per the press reports, MeitY is expected to release the final "Drat Rules for Public Comments" in the second week of August. In the meantime, the "Interim Draft Rules for comments from select group" had been in circulation.

FDPPI collected public views on this "Interim Draft Rules" during a day long event in Bengaluru on July 27.

As and when the "Final Rules" become available, we will hold industry consultation again and submit the "Voice of the Industry". In the meantime, we are submitting the views based on the Interim draft rules so that these views can be considered before the final rules are released.

These comments are provided on each of the 20 rules and 7 schedules that were part of this "Interim Draft Rule" document.

Copy of the rules used for this discussion is available at www.dpdpa.in/dpdpa_rules

Comments

Rule No	Comments
1	It is noted that the notification is restricted to those Rules related to constitution of DPB. There is a need to specify the timelines both for the DPB to go into action and the time when penal provisions of the Act will become effective. It is recommended that the notification shall prescribe that DPB shall be formed within 3 months of first notification or the zero date. Compliance shall be required before 9 months and penalties shall become effective after one year. Section 44 DPDPA 2023 should be specially mentioned as becoming effective after one year so that Section 43A of ITA 2000 (Information Technology Act-2000) will be replaced only after the penalty clauses under DPDPA 2023 becomes effective.

	Provisions related to Section 10 for registration of identified significant data fiduciaries [a separate rule for identification of Significant data fiduciaries as per Section 10(1) is required] should become effective within 6 months from zero date which is 3 months after formation of DPB. Provisions of 10(2)(a) [DPO] should also be effective within 6 months and provisions of 10(2) (b) [Data Auditor] and 10(2)(C) [DPIA] from the financial year 2025-26. There is a debate on whether there should be a classification of Significant Data Fiduciaries into different categories (SMEs, Social Media Intermediaries etc) and provide different timelines of implementation. This is not essential, and the need can be incorporated through voluntary forbearance of DPB in imposing penalties.
2	**Definitions:** **Sensitivity** It is necessary to define the concept of "Sensitivity" to identify the Significant Data Fiduciaries and guide the DPB in determining the penalties. Such sensitivity should incorporate the "Harm" to the data principal and include "Manipulation of mental and neural behaviour of a data principal". To define "Significance" of a data fiduciary, "Sensitivity" needs to be defined. To define "Sensitivity", "Harm" should be defined. Definition of "Harm" is the missing link of this law to "Privacy". **"Consent Artifact"** The details presently provided under the definition clause are to be part of the rule. It suffices to say "Consent Artifact" is an electronic record/instrument to issue a notice as per Section 5 and receive consent as per Section 6 of the Act. **Personal Data Breach Artifact** The details presently provided under the definition clause are to be part of the rule. It suffices to say "Personal Data Breach Artifact" is an electronic record/instrument to issue a notice as per Section 8(6) of the Act. There is no need to provide definitions of "Digital Locker Service Provider" , Electronic record, electronic signature, intermediary etc which are part of ITA 2000 definitions or definitions in the DPDPA 2023 itself. Rule 2(2) will take care of such terms. Only terms relevant to providing clarity to the rules which are not defined in ITA 2000 or DPDPA 2023 need to be specified.

	The definition of an "App" may require to be expanded as "App means an electronic program containing a group of instructions for achieving a specified function either on a computer or a Mobile or any other computing device". "Nomination" should be defined as "an instruction for transferring the custody of personal information of a data principal from a data fiduciary to another designated person on the event of death of a data principal or on termination of the processing for any reason". "Nominee" should be defined as "A person, individual or otherwise who is authorized by the data principal to whom the custody of the personal data of the data principal may be transferred after his death for disposal as per law of inheritance applicable to an actionable claim. There may be need for adding definitions such as "Archival" of personal data as distinct from "Deletion" along with definition of "National Archival of Personal Data" and "Unclaimed Personal Data". It is preferable to also add a definition of "Anonymisation" as distinct from "Pseudonymisation" or "De-identification". It is also preferable to add a definition of "Business Contact Data" with a specific note that it is not considered "Personal Data". It is also necessary to define "Unclaimed Data" to support the nomination rules. It is also necessary to define "Disputed Data" where the data principal may want correction or deletion but the Data Fiduciary and DPB is not agreeable. While defining a "Data Fiduciary" in an organization where members of the organizations act as independent consultants, it is necessary to indicate that the individual members constitute "Joint Data Fiduciaries" of the Principal Data Fiduciary. This is consistent with the HIPAA where hospital is a covered entity and individual doctors other than employees are also considered Covered entities. This system applies to Hospitals with consulting doctors, Law Firms or CA firms with members acting both independently and jointly. There are also situations where a Data fiduciary is a Group of Companies with subsidiaries and connected companies. A provision can be considered to enable them to declare themselves as a "Group Data Fiduciary" so that they can appoint a common DPO.
3	**Notice for Prospective Collection:** In rule 3(1)(b), "Purpose" should be the first point and "Itemised description" should be the dependent second point. "Itemised description" should specify "Such personal data that is required for the specified purpose. (Takes care of the Data Minimization principle).

	It may be specified that "Nomination" can be a point that can be indicated in the notice. A separate rule for "Nomination" is required to be provided as discussed subsequently in this note. The "Model Notice" under Schedule I needs to be dropped since it is misleading and does not cover the requirements that need to be customised. Rule 3(2) may be dropped since State and its instrumentalities have the "Legitimate Use" option and the proposed rule only speaks of existing beneficiaries and does not cover new beneficiaries. Alternatively, the rule 3(2) can mention "Subject to the use of the legitimate use option as per Section 7(b), the State or its instrumentalities may also seek consent as per para (1) above. Provision should be made for exceptions such as a "Consent for discovery of purpose", "Profiling for Marketing purpose" and "Monetization" and shall be obtained with a verifiable witness. (Details of such definition may be suggested if required)
4	**Notice for Legacy Data:** In this rule there should be specific provisions for "Inability to serve notice due to lack of contact information or failure of contact", through a notification on the website of the organization and in newspaper/virtual notice. It is suggested that DPB may set up an exclusive website for Cyber Notices as part of DPDPA Rules and designate it for providing general notices to data principals. This site need to be rendered in multiple languages and DPB may provide publicity to this. There should be a specific mention that non receipt of consent within a time of one year from the date of notice shall be considered as withdrawal of consent which should be followed by stoppage of processing and secured archival of the personal data. The data shall not be deleted without specific verifiable consent. The need for "Renewal of Consent" should be applicable for all personal data presently being processed unless otherwise covered under legitimate use or exemptions under the Act and not limited to "Where a data principal has given consent."
5	**Consent Manager** The Rule on Consent Manager requires some modifications. The definition of Consent Manager under DPPDA 2023 should be distinguished from the definition of Consent Manager under the Account aggregator scheme.

At present MeitY seems to be restricting itself to the concept in its own DEPA architecture where the term "Consent Manager" (CM-DEPA) was introduced as a technology platform. This was meant for the limited purpose of data users like portfolio managers etc requesting for consent for financial management purpose and such requests were forwarded to data givers like Banks who could provide the information. This would relieve the service user from filling up long forms including assets and liabilities, KYC information etc besides demographic information from time to time. RBI applied this system in the account aggregator scheme. These use cases are meant to be used for creation of a new account by the financial service provider and not meant for repeated use.

The Consents under DPDPA 2023 are multiple type of consents, required repeatedly for different sets of data elements by different types of data fiduciaries. It includes the financial service providers such as account aggregators and Amazon or Zomato type of data fiduciaries who may require one set of data for clearance of payments and another limited set for logistics.

The CM-DEPA system envisages that every consent request is received from a data fiduciary, referred to the data principal, consent received and then information sent to the data fiduciary. For every purchase from Amazon and for every order of food from Zomato, separate notice and consent is required.

In the ordinary course, a data principal goes to a data fiduciary service site and receives the notice which he clicks for acceptance. The data goes directly from the data principal to data fiduciary as part of the order.

In the CM-DEPA scheme, the data principal goes to the data fiduciary site and when he tries to place the order, the data fiduciary refers to the CM-DEPA with some identity of the data principal. The data then comes back to the data fiduciary. In the process, there is an identification verification by the CM as well as an extra leg of sending a request to the CM and obtaining the information while the data principal waits for the confirmation of the order.

This is inefficient, additional data consuming and involving an additional identity verification process.

In this process, the CM-DEPA does not have any visibility of the data and if the platform is suitably configured, data flows in and out like an ISP. It is therefore an "Intermediary" under ITA 2000.

The CM-DPDPA was not conceived to be the replica of this CM-DEPA since it was necessary to address two problems namely the Consent Fatigue and Language barrier and technology understanding barrier in providing consent.

The CM-DPDPA was therefore considered as an entity who can represent the data principal with the data fiduciary for not only providing the consent on demand but

	also for withdrawal of consent or raising any grievance. Hence CM-DPDPA was conceived as a "Trustee of the Data Principal" and not as a simple ISP type intermediary. CM-DPDPA could therefore have visibility to personal data, he could filter the data for delivery to a particular purpose and challenge the permissions with his superior technical and language capability to avoid dark patterns or misleading permission requests. He could use anonymization and pseudonymisation if required and deliver only such data as is required for a purpose. For example, amazon order placement team may get the financial information which is normally shared with the payment gateway but not the demographic or locational data (unless they justify the requirement for appropriate reasons). The amazon or Zomato delivery team would only get the information about the delivery address and not the other details and they can share it with any logistic company. The data principal is relieved of the need to check the permissions and whether a particular data element requested is reasonably required for the purpose or not. If the concept of CM-DPDPA is merged with CM-DEPA, this advantage would be given up. The Consent Manager provision in DPDPA 2023 was innovative and like the "Copyright Society" in Copyright law could be considered as an instrument through which Privacy Culture can be built up in the Country and data principals could be helped in protecting their privacy against business which is driven by their profit motive. We strongly believe that this great opportunity should not be missed. Hence a review of Section 5 as suggested. Even this system requires the "Fit and Proper Criteria" and hence many of the current provisions are relevant. However, Rule 3(a) needs to be modified to remove the words "Without the consent manager being in a position to access the personal data" In as much as every "Significant Data Fiduciary" is allowed to sub-contract their work with responsibility, the need to prevent "Consent Manager" from sub-contracting can be reviewed. On the other hand, it may be specified that every Data Processor of a Consent Manager would be deemed to be a Significant Data Fiduciary himself. It shall be made mandatory that when a Consent Manager needs to exit or is suspended or services cancelled, the service shall be ported to another licensed Consent Manager so that the data principal is not inconvenienced. Such porting shall

	be approved by DPB. Alternatively, a time of up to 1 year should be provided for the data principals to switchover to another consent manager of his choice. The rules prescribe that CM-DPPDA shall be a company but not a "Foreign Company". As per Companies Act, *—foreign company means any company or body corporate incorporated outside India which— (a) has a place of business in India whether by itself or through an agent, physically or through electronic mode; and (b) conducts any business activity in India in any other manner.* This definition is restricted to "Incorporation outside India" and is not sufficient to prevent data laundering by consent managers where they set up a consent manager, collect personal data and sell off the company to a foreign entity. CIBIL-Trans Union is a living example of such a methodology. "Data" is a sovereign asset, and it must be protected from being stolen or surreptitiously laundered. Hence the definition of "Foreign Company" should be expanded to include any foreign or non-resident shareholding that exceeds 10% or controlling interest that 33% of the members of the Board. If the Consent Manager is only a platform and every consent must be approved by the Data Principal, the very purpose of the consent manager to relieve the consent fatigue and difficulty in understanding the permission requirements is defeated. The CM should therefore be a "Power of attorney holder" who can take some decisions on his own without disturbing the data principal. It is also suggested that the rules should prescribe that Consent manager shall not store personal data abroad nor controlling interest be transferred to an entity which is located outside India.
6	**Processing by State** The section 7(b) of the Act refers to processing of personal data by the State for issuing subsidy, benefit, service, certificate, license or permit where there has been a previous valid consent. This rule re-iterates the narration of the section and adds a Schedule II for further clarification. The section 7(b) has brought processing in this context when there has been a previous consent under "Legitimate use". The Schedule II recognizes this by making a reference to the earlier consent. 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 details of this rule are contained in Schedule III and refers to Section 8(7)(a) relating to erasure of data on expiry of the process for which it was provided after a certain period of inactivity. It is more like a "Limitation Period" after which the data becomes eligible for "Deletion" or "Archival". 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 in Schedule III 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 two crore registered users in India. Clarity should be provided regarding other types of data fiduciaries and those having less than 2 crore subscribers in India.

	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. This may be added in the definition clause so 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. The use of the term "Business Contact" indicates that an individual can have personal data as well as "Business Contact Data" separately. Obviously, Business Contact data is not personal data to which the conditions like consent are applicable. The rules however do not provide such clarification which would have been useful.
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 Schedule IV 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 thee "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. The biggest gap in the rules is however that it has not defined the way an organization can be identified as a "SDF". The Act does mention the words "Sensitivity" of personal data processed and "Risk to the rights of Data Principal". There is no mention of these terms in the Rules. The "Volume" of the personal data processed for the purpose of this section needs to be indicated. 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. The rule at present should publish some criteria for determining a DF provisionally as an SDF and require them to apply to DPB with information on their activity. 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	**Research and Statistical Purpose** Under this rule and schedule V, organizations for whom data may be transferred for research, archiving and statistical purposes have been indicated. Under this rule it would have been possible to have defined the "de-identification", "Pseudonymisation" and "Anonymisation" standards so that they could have been linked to the permitted disclosures under this rule. The rule need to be expanded with the definition of these terms and making it as a pre-requisite to be transferred to the agencies indicated for research or other purposes.
15	**DPB Constitution** This rule refers to Section 19 of DPDPA 2023 under which Government could have notified the number of members to be appointed to the DPB. It is suggested that the rule mentions that a total of seven members may be appointed to the Board over the period of next one year when the act is implemented in stages.
16	**Salaries and Allowances of Chairman and Members** This rule provides a schedule VI detailing the salary and allowances of the Chairman and the members of the DPB as well as the service conditions. There are no comments.
17	**Proceedings of DPB** This rule details the way proceedings of the Board may take place and how the orders, directions and instruments would be authenticated. There are no comments
18	**Service terms for officers** This rule details the Terms and conditions of appointment and service of officers and employees of the Board. Schedule VII provides the full details. There are no comments
19	**Techno Legal measures to be adopted by the Board** This rule details the Techno Legal measures to be adopted by the Board in its functioning**.** The rule provides the usage of SEBI's SMARTODR platform for mediation.

	However, this platform has no expertise at present on resolving data protection disputes and there is no provision to empanel data protection professionals to the platform. A complete guideline for this purpose needs to be provided. Additionally, DFs may be provided an option to use any other mediation facility if the Mediators are accredited to DPB for their expertise and knowledge in Data Protection area. The dispute resolution mechanism for data principals to claim personal remedy as well as remedies for some of the Data Fiduciary vs Data Processor disputes (refer Section 72A of the Information Technology Act) fall under the jurisdiction of the Adjudicator under the Information Technology Act. This has to be prominently indicated in the Privacy Notice for the information of the data principals. A mention can be made about the need to approach the Adjudicator of Information Technology act where required and for DPB to make a reference either to the Adjudicator or to any criminal investigation agency when it becomes aware of the need during its investigation.
20	**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.