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

13th February 2025

Comments on the Draft Rules released for selective discussion

To

The Secretary
MeitY
New Delhi

Dear Sir

This has reference to the notification of January 3, 2025 related to the draft rules on DPDPA.

These comments are submitted from FDPPI (Foundation of Data Protection Professionals in India) which is a premier independent organization (Section 8 Company) promoted by individual data protection professionals and not aligned with any Big Tech Companies nor organizations representing any vested interests in India or abroad, submits the following comments

FDPPI has collected public views on this "Draft Rules" through its interactions with industry representatives both through physical meetings and through virtual interactions.

We request that the comments and suggestions made here in may kindly be considered for incorporation in the final version of the rules.

Part A: General Comments

The law of DPDPA 2023 is already in place and is immutable at this point of time. It is noted that the current exercise is only for fine tuning of the published draft rules.

Hence our comments presume that the law as it has been notified stands as the fundamental document of reference and the comments are only related to the draft rules as are considered feasible under the enacted law.

It is recognized that in the event of any rule exceeding the basic character of the provision of the law to which it refers to, there could be a challenge on the legal validity of the rules as being ultra-vires the law.

For the same reason, FDPPI expects that the rules may be brief, precise and only cover the essential clarifications without the detailing like a Check list or recommending any specific tool or technology for implementation.

It is understood that the industry would exercise due diligence in implementing the law along with the minimum detailing available in the rules. If and when the industry is negligent and does not observe due diligence, the consequences would reflect in the decisions of the inquiry following a registration of a complaint or a Suo-moto inquiry.

Because of the delays in the implementation of the Data Protection law in the past, the industry has developed a complacence that the law will not come into force for some more time and DPB will not be functional for a few more years and even when it is functional, it will be toothless and lenient on the industry.

It is necessary to remove this complacency by MeitY and DPB ensuring that quick penal action is initiated on a few delinquent companies at the earliest and there should not be any more delays. Further even if time is given for penalties, the "Notification of Data breach" to the DPB may be mandated retrospectively from 11th August 2023. For this purpose, even before the penalty may be made effective after some time, DPB should put certain companies on "DPDPA Watch List" so that such companies can recognise the need for improving their compliance status.

Part B: Clause by Clause Comments on the published draft rules

As per the Section 40 of the Act, 25 specific rules were required to be notified under different sections apart from the empowering "any other matter which may be prescribed". The 22 rules and the 7 schedules cover all the requirements that are necessary. The following comments try to register our comments on the sufficiency and excessive aspects of the rules if any along with a few suggestions.

Comments

Rule No	Comments
1	It is noted that the notification of the date of effect of the Act as of now is restricted to those Rules related to constitution of DPB. Time schedule for other requirements is to be specified by a separate notification/s in consultation with the DPB after its formation. It is recommended that the following additional time lines are prescribed for different aspects of implementation to provide a clear schedule of implementation to the industry. a) The DPB shall be formed within 3 months of this notification and commence its operational website within 4 months of the notification. b) Provisions related to Registration of Consent Manager shall commence as soon as the DPB becomes operational. c) Compliance requirements such as Consent, Data Breach Notification and Restrictions on transfer of data outside India (Where applicable) shall be required before 9 months from the notification.

	d) Penalties under Section 33 shall be effective after one year from notification. (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 shall be 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 9 months from the date of notification. g) All other residual requirements under the Act shall be deemed applicable at the end of one year from notification. h) Non Corporate Data Fiduciaries and those who fall under the category of SME/MSME shall be provided an additional time of 6 months over and above the time given for other entities for each of the different provisions.
2	**Definitions:** Removal of the definitions is welcome since it avoids the rule defining new terms not in the original Act which may be considered as "Excessive".
3	**Notice to be given to the Data Principal:** **Legacy Data Principals** A mention may be made that notice in the same format (as per rule 3) is required to be sent to all legacy data principals within 3months of the notification. a) Where the Data Fiduciary does not possess valid email or SMS contact information, a notice shall be published through a general advertisement in one English and one Prominent local language newspaper without the need for specifying the data principals but specifying the details of the purpose for which the legacy data with the data fiduciary may be used along with the data retention requirement. 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) The notice shall indicate that where no valid response is received from the legacy data principal within one month to continue processing, all instances of the data of the data principal in the custody of the data fiduciary shall be de-commissioned and subsequently archived for deletion including instances in the back up. d) Such data for which no response is received shall be deleted or anonymised after 6 months subject to one reminder at the end of 3 months followed by a second reminder before 48 hour 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.

	Custody of such data shall be retained with a distributed control mechanism under the control of custodians which include non-Government persons. 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. The archive may be de-classified after a period of 12 years. The custody of the National archive with a distributed cryptographic key management system including non-government persons (similar to the DNS Root Server access key management of ICANN) shall ensure that the data may not be misused by any of the custodians including the Government.
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 stringent "Fit and Proper" criteria is not necessary and may be substantially removed. 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. 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.

	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 is not necessary. Hence the provision of retention for seven years may be removed and replaced by " as long as retained by the data fiduciary". Simultaneously, it may be prescribed that the data fiduciary who has received a consent through a consent manager and intends to stop processing and delete the data shall notify the consent manager of such deletion. c) All Consent Managers registered with DPB shall be declared ab-initio as "Protected Systems" under Section 70 of Information Technology Act 2000 and necessary controls under the oversight of CERT-In shall be in-place. d) 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 may be removed.
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. (eg: when data access is compromised within the organization from one employee to another). 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) Personal Data Breach not resulting in exfiltration or modification of data c) Personal Data Breaches resulting in exfiltration or modification of data The rules should treat these differently. It is necessary to recognize that every personal data breach involving loss or damage to data creates a liability under Section 43 of ITA 2000 and is also a data breach reportable under CERT IN guidelines even after the repealing of Section 43A. There should be a process where the DPB and CERT IN act in harmony dealing with the Personal data 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 created by MeitY which may specify that the ITA 2000 Compliance Manager and DPDPA Compliance Managers designated by MeitY shall jointly resolve Personal Data Breach related conflicts between CERT IN and DPB if any. 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. 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 simultaneous change in the CERT IN rules related to data breach while these rules are being notified. Suggestions are: 1. Provisional Personal Data Breach shall be reported only to DPB immediately on being aware. Confirmed data breach involving exfiltration or modification of personal data shall be reported to the data principal as soon as the data fiduciary becoming aware of the "Confirmed Data Breach" 2. All Data Breaches recorded since 11th August 2023 may be reported to DPB under the powers of Section 36 of DPDPA 2023 3. Detailed Report within 72 hours or as extended shall be submitted as proposed to the DPB. 4. A notification of the report sent to DPB on the website of the Data Fiduciary should be mandatory. 5. A link to the detailed report should be sent to the Data Principals through e-mail or SMS where available
8	**Erasure of Personal Data** The details of this rule as mentioned in the third schedule 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 "Decommissioning and Archival". The term "Decommissioned Data" should 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. Such data should be "De-commissioned and 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, Data Fiduciaries 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.

	Appropriate security procedures may be prescribed for distributed custody of such data on the lines of ICANN procedure for root server key management. 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". It should be part of the due diligence of an organization to determine when the data needs to be deleted whether 3 years or less irrespective of whether they hold 2 crore data or less.
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 it shall be the choice of the data principal to declare a data as personal or for business contact and such data shall be treated as "Non Personal Data" for the purpose of other provisions of the Act.
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 guardian identification" with reference to the name of the parent in the Aadhaar card of the minor. Ministry should 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" problems 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. There is a need to have a designated official as provided under Rule 22 for approving any institution other than what is indicated under the Fourth Schedule for similar exemption.
12	**Significant Data Fiduciary** a) 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.

b) 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 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.

c) 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.

d) 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 from within the organization and take the assistance of a DPO from outside in case necessary.

e) Further the expected credentials of the DPO and Data Auditor could be indicated at least in broad terms as "Being Conversant with the Indian Data Protection law" .

f) 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.

Alternatively, the volume criteria can be left out completely and it may be left to the "Due Diligence" of the organization to determine whether the organization self declares itself as a "Significant Data Fiduciary" or not.

g) 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.

h) 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 register of such entities may be maintained by the designated official under Rule 22.

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.

The "Designated official" under Rule 22 may maintain a register of "Significant Data Fiduciaries" including self declared entities and introduce a procedure for online registration of such entities.

i) 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".

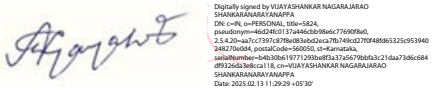
	The process-based compliance is essential since the collection of personal data is also process dependent and data minimization, data retention minimization and purpose definitions may all be linked to a process rather than the entity. j) Considering the many doubts that the implementers of the Act may 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.
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. a) 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. In the absence of an identity provided by the data principal in the original consent or a digital signature or a new KYC, the possibility of providing any information at the request of a person claiming to be a data principal is a security risk. The Rule may provide that the Data Fiduciary shall exercise "Due Diligence" in identifying the data principal before accepting the request for exercising the Rights. b) 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. c) 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. This "National archive" may be declared as the "Nominee by Default". The archive shall be secured by a distributed security management system similar to ICANN managing the Domain Name Root Server security. Required provisions may be made in this regard separately.

	d) 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, it is recommended that the rules may define "Nomination of Personal Data" as "Transfer of custody of personal data of the deceased data principal", the means of confirming the information of death and the means of transferring the safe custody before deleting it from the custody of the data fiduciary. 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.(as recommended). Under this suggested process, the personal data of the deceased data principal may be securely handed over to the Custodian of the "Archive of Personal data of a Deceased Data Principal") 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** Under this rule, conditions for transferring personal data to organizations for archiving and statistical purposes have been indicated. It includes the generally accepted privacy principles and reasonable security. There are no specific comments.
16	**DPB Constitution** This rule refers to Section 19 of DPDPA 2023 and the following comments are recommended. a) The minimum number of members (excluding the chairman) shall be Six and Maximum shall be Twenty. b) DPB shall commence its operation with the minimum number of members and MeitY shall review the requirement of the DPB once in a year and increase the number of members as required. c) The Search Committee may function for one year at a time and shall review the functioning of the DPB annually and submit a report to the MeitY before a new Search Committee is set up for the following year. d) The respective Search Committee shall be responsible for evaluating any complaints received against the Chairman/Members or observations recorded during the monitoring of the activities of the DPB and recommend disqualification if required.

	e) The Search Committee shall meet each quarter or as often as otherwise required to review the activities of the DPB and recommend corrective action if necessary. f) The external members of the search committee may be paid remuneration as may be determined by the Ministry for the services rendered including sitting fees for meetings. g) The external members of the Search Committee shall retire each year and shall not be eligible for re-appointment for a continuous second term.
17	**Salaries and Allowances of Chairman and Members** This rule provides a detailing the salary and allowances of the Chairman and the members of the DPB as well as the service conditions. There are no comments.
18	**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
19	**Functioning of the Board as a Digital Office** This rule suggests the use of digital means of conducting the affairs of the DPB and the following recommendations are submitted a) The DPB digital office and connected data resources shall be declared as "Protected System under Section 70 of ITA 2000. b) All data of the DPB shall be kept in its own data centers and shall not be outsourced. c) The Security of the DPB shall be the responsibility of the CERT-IN
20	**Service terms for officers** This rule details the Terms and conditions of appointment and service of officers and employees of the Board. Schedule VI provides the full details. There are no comments
21	**Appeal to Appellate Tribunal** The Act refers to Sections 14A, 16 and 18 of the Telecom Regulatory Authority of India 1997 in respect of the appeals to be filed against the decision of the DPB. However, the Act does not mandate that the TDSAT shall be the appeal authority. Hence Rule 21 shall specify that a) The Telecom Disputes Settlement and Appellate Tribunal shall be the designated Appellate Tribunal for the time being until a separate tribunal is set up as required.

	b) The procedure for filing the appeal and resolution of the appeal shall be determined by the designated Appellate Tribunal. c) The appellate Tribunal shall make its inquiry report available to the Adjudicator of Information Technology Act or a competent court to which the data principal may approach for any compensation arising out of the contravention of DPDPA 2023 by any entity.
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. Further it is recommended that a) The officials designated under this Rule shall be appointed to be operational within 1 month from the notification. b) The official designated for carrying out assessment for notifying any data fiduciary or class of data fiduciary as a "Significant Data Fiduciary" shall also notify data fiduciaries under Section 17(3) on specific applications for exemptions.

Yours sincerely



Na.Vijayashankar

Chairman

FDPPI