C.A.S.C.A

DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

Response to Public Consultation Drive by Ministry of Electronics and Information Technology

March, 2025

DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

COMMENTS AND SUGGESTIONS

Authors: Chirkankshit Bulani, Sanskriti Bishnoi, Vishwaroop Chatterjee, Kunaal Hemnaani, R Dayashakti, Amishi Jain, Raima, Shoptorishi Dey, Sanskriti Koirala, Swastika Chowdhury, Aadit Seth, Shantanu Singh, Eknoor Kaur, Tarush Saitia, Jacob Eldho Kalarikkal, Uday Gupta, Aarav Singh

Inputs: Dr Ivneet Walia, Registrar (Officiating), Rajiv Gandhi National University of Law, Patiala.

CENTRE FOR ADVANCED STUDIES IN CYBER LAW AND ARTIFICIAL INTELLIGENCE [CASCA] is a research-driven centre at RGNUL dedicated to advancing scholarly research and discourse in the field of Technology Law and Regulation. As a research centre of a leading institution in India, we are committed to promoting interdisciplinary research, fostering collaboration, and driving innovation in the fields of cyber law, artificial intelligence, and other allied areas.

For more information
Visit **cascargnul.com**

TABLE OF CONTENTS

TABULAR STATEMENT ON THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

Section	Column 1: Proposed Rule	Column 2: Our Recommendations
(**Rule 2**) *r/w* **Section 2 of Digital Personal Data Protection Act, 2023**	*Section 2(h) of Digital Personal Data Protection Act, 2023 - "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.* *Section 2(x) of Digital Personal Data Protection Act, 2023 - "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.* *Section 2(z) of Digital Personal Data Protection Act, 2023 - "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10.*	*Section 2(h) of Digital Personal Data Protection Act, 2023 - "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.* *Section 2(x) of Digital Personal Data Protection Act, 2023 - "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.* *Section 2(z) of Digital Personal Data Protection Act, 2023 - "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10 OR Data Fiduciaries who*
(**Rule 3**)	*Notice given by Data Fiduciary to Data Principal.—The notice given by the Data Fiduciary to the Data Principal shall— (a) be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary; (b) give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data*	*Notice given by Data Fiduciary to Data Principal.—The notice given by the Data Fiduciary to the Data Principal shall— (a) be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary; (b) give notices, in clear and plain language, specific to businesses which adhere to their data processing requirements.*

(**Rule 4**)	*4(2) On receipt of such application, the Board may make such inquiry as it may deem fit to satisfy itself regarding fulfilment of the conditions set out in Part A of First Schedule, and if it— (a) is satisfied, register the applicant as a Consent Manager, under intimation to the applicant, and publish on its website the particulars of such Consent Manager; or (b) is not satisfied, reject the application and communicate the reasons for the rejection to the applicant.* *4(3) The Consent Manager shall have obligations as specified in Part B of First Schedule.* *4 (4) If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under this rule, it may, after giving an opportunity of being heard, inform the Consent Manager of such non-adherence and direct the Consent Manager to take measures to ensure adherence.*	*4(2) On receipt of such application, the Board may make such inquiry as it may deem fit to satisfy itself regarding fulfilment of the conditions set out in Part A of First Schedule, and if it— (a) is satisfied, register the applicant as a Consent Manager, under intimation to the applicant, and publish on its website the particulars of such Consent Manager; or (b) is not satisfied, reject the application and communicate the reasons for the rejection to the applicant ; c) the board shall process applications for registration of a Consent Manager within a period of 60 days from the date of receiving an application.* *4(3) The Consent Manager shall have obligations as specified in Part B of First Schedule.* *4(4) If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under this rule, it may, after giving an opportunity of being heard, inform the Consent Manager of such non-adherence and direct the Consent Manager to take measures to ensure adherence. The board shall conduct a periodic review of the obligations of Consent Managers at intervals not exceeding 12 months.*
(**Rule 5**)	*(1)The State and any of its instrumentalities may process the personal data of a Data Principal under clause (b) of section 7 of the Act to provide or to issue to her any subsidy, benefit, service, certificate, licence or permit that is provided or issued under law or policy or using public funds.* *(2) Processing under this rule shall be done following the standards specified in Second Schedule.* *(3) In this rule and Second Schedule, the reference to any subsidy, benefit, service,*	*(1)The State and any public authorities may process the personal data of a Data Principal under clause (b) of section 7 of the Act to provide or to issue to her any subsidy, benefit, service, certificate, licence or permit that is provided or issued under law or policy or using public funds.* *(2) Processing under this rule shall be done following the standards specified in Second Schedule.* *(3) In this rule and Second Schedule, the reference to any subsidy, benefit, service,*

	certificate, licence or permit that is provided or issued— *(a) under law shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit in exercise of any power of* *or the performance of any function by the State or any of its instrumentalities under any law for the time being in force;* *(b) under policy shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit under any policy or instruction issued by the Central Government or a State Government in exercise of its executive power; and* *(c) using public funds shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit by incurring expenditure on the same from, or with accrual of receipts to,—* *(i) in case of the Central Government or a State Government, the Consolidated Fund of India or the Consolidated Fund of the State or the public account of India or the public account of the State; or* *(ii) in case of any local or other authority within the territory of India or under the control of the Government of India or of any State, the fund or funds of such authority.*	*certificate, licence or permit that is provided or issued—* *(a) under law shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit in exercise of any power of* *or the performance of any function by the State or any public authorities under any law for the time being in force;* *(b) under policy shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit under any policy or instruction issued by the Central Government or a State Government in exercise of its executive power; and* *(c) using public funds shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit by incurring expenditure on the same from, or with accrual of receipts to,—* *(i) in case of the Central Government or a State Government, the Consolidated Fund of India or the Consolidated Fund of the State or the public account of India or the public account of the State; or* *(ii) in case of any local or other authority within the territory of India or under the control of the Government of India or of any State, the fund or funds of such authority.*
(**Rule 6**)	*(1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum,—* *(a) appropriate data security measures, including securing of such personal data* *through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data;*	*(1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards appropriate and proportionate to the risk and sensitivity of the data to prevent personal data breach, which shall include, at the minimum,—* *(a) appropriate data security measures, including securing of such personal data* *through its encryption, obfuscation or masking*

	(b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor; *(c) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;* *(d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of databackups;* *(e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;* *(f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards; and* *(g) appropriate technical and organisational measures to ensure effective observance of security safeguards.* *(2) In this rule, the expression "computer resource" shall have the same meaning as is assigned to it in Information Technology Act, 2000 (21 of 2000).*	*or the use of virtual tokens mapped to that personal data;* *(b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor;* *(c) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;* *(d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of databackups;* *(e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;* *(f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards; and* *(g) appropriate technical and organisational measures to ensure effective observance of security safeguards.; and* *(h) a mechanism to test, analyse and evaluate the security safeguards every six months.* *(2) In this rule, the expression "computer resource" shall have the same meaning as is assigned to it in Information Technology Act, 2000 (21 of 2000).* *(3) "Minimum security measures" and "appropriate technical and organisational measures" (under sub-section G) including but not limiting to encryption, pseudonymisation, ensure confidentiality and access control, obfuscation and masking.*

(**Rule 7**)	*(1) On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary,—* *(a) a description of the breach, including its nature, extent and the timing and location of its occurrence;* *(b) the consequences relevant to her, that are likely to arise from the breach;* *(c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk;* *(d) the safety measures that she may take to protect her interests; and* *(e) business contact information of a person who is able to respond on behalf of theData Fiduciary, to queries, if any, of the Data Principal.* *(2) On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board,—* *(a) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact;* *(b) within seventy-two hours of becoming aware of the same, or within such longer period as the Board may allow on a request made in writing in this behalf,—* *(i) updated and detailed information in respect of such description;* *(ii) the broad facts related to the events, circumstances and reasons leading to the breach;* *(iii) measures implemented or proposed, if any, to mitigate risk;* *(iv) any findings regarding the person who caused the breach;* *(v) remedial measures taken to prevent recurrence of such breach; and*	*(1) On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, within twenty-four hours, through her user account or any mode of communication registered by her with the Data Fiduciary,—* *(a) a description of the breach, including its nature, extent and the timing and location of its occurrence;* *(b) the consequences relevant to her, that are likely to arise from the breach;* *(c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk;* *(d) the safety measures that she may take to protect her interests; and* *(e) business contact information of a person who is able to respond on behalf of the Data Fiduciary, to queries, if any, of the Data Principal.* *(2) On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board,—* *(a) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact;* *(b) within seventy-two hours of becoming aware of the same, or within such longer period as the Board may allow on a request made in writing in this behalf,—* *(i) updated and detailed information in respect of such description;* *(ii) the broad facts related to the events, circumstances and reasons leading to the breach;* *(iii) measures implemented or proposed, if any, to mitigate risk;* *(iv) any findings regarding the person who caused the breach;* *(v) remedial measures taken to prevent recurrence of such breach; and*

	(vi) a report regarding the intimations given to affected Data Principals. *(3) In this rule, "user account" means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary*	*(vi) a report regarding the intimations given to affected Data Principals.* *(c) The Data Fiduciary shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall made available to the board at any time to verify compliance.* *(3) In this rule, "user account" means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary*
(**Rule 9**)	*Contact information of person to answer questions about processing.—Every Data Fiduciary shall prominently publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data.*	*Contact information of person to answer questions about processing.—Every Data Fiduciary shall prominently publish on its website and/or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business current contact information, including email and phone number, of the Data Protection Officer, if applicable, or a designated person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of their personal data in a reasonable time and manner.*
(Rule 10)	*(1) A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to—*	*(1) A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent or a person entrusted with the lawful guardianship of the child or a person with disability, is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent or lawful guardian, is an adult who is identifiable if required in connection with compliance with*

	(a) reliable details of identity and age available with the Data Fiduciary; or *(b) voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued by an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.* *(2) A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, a designated authority or a local level committee, under the law applicable to guardianship.* *(3) In this rule, the expression—* *(a) "adult" shall mean an individual who has completed the age of eighteen years; (b) "Digital Locker service provider" shall mean such intermediary, including a body corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000);* *(c) "designated authority" shall mean an authority designated under section 15 of the Rights of Persons with Disabilities Act, 2016 (49 of 2016) to support persons with disabilities in exercise of their legal capacity;* *(d) "law applicable to guardianship" shall mean,—* *(i) in relation to an individual who has long*	*any law for the time being in force in India, by reference to—* *(a) reliable details of identity and age available with the Data Fiduciary; or* *(b) voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued by an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.* *(2) The Data Fiduciary must ensure that the person providing consent for the data processing of the child, is the parent or the legal guardian of the child and the parent or the legal guardian is identifiable.* *(3) A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, a designated authority or a local level committee, under the law applicable to guardianship.* *(4) In this rule, the expression—* *(a) "adult" shall mean an individual who has completed the age of eighteen years; (b) "Digital Locker service provider" shall mean such intermediary, including a body corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000);* *(c) "designated authority" shall mean an authority designated under section 15 of the Rights of Persons with Disabilities Act, 2016*

	term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who despite being provided adequate and appropriate support is unable to take legally binding decisions, the provisions of law contained in Rights of Persons with Disabilities Act, 2016 (49 of 2016) and the rules made thereunder; and *(ii) in relation to a person who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of such conditions and includes a person suffering from severe multiple disability, the provisions of law of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999) and the rules made thereunder;* *(e) "local level committee" shall mean a local level committee constituted under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999);* *(f) "person with disability" shall mean and include—* *(i) an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions; and* *(ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes an individual suffering from severe multiple disability.*	*(49 of 2016) to support persons with disabilities in exercise of their legal capacity;* *(d) "law applicable to guardianship" shall mean,—* *(i) in relation to an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who despite being provided adequate and appropriate support is unable to take legally binding decisions, the provisions of law contained in Rights of Persons with Disabilities Act, 2016 (49 of 2016) and the rules made thereunder; and* *(ii) in relation to a person who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of such conditions and includes a person suffering from severe multiple disability, the provisions of law of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999) and the rules made thereunder;* *(e) "local level committee" shall mean a local level committee constituted under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999);* *(f) "person with disability" shall mean and include—* *(i) an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions; and* *(ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and*

		includes an individual suffering from severe multiple disability.
(**Rule 11**)	*(1) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child by such class of Data Fiduciaries as are specified in Part A of Fourth Schedule, subject to such conditions as are specified in the said Part.* *(2) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child for such purposes as are specified in Part B of Fourth Schedule, subject to such conditions as are specified in the said Part.*	*(1) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child by such class of Data Fiduciaries as are specified in Part A of Fourth Schedule, subject to such conditions as are specified in the said Part, provided that such processing complies with the well-being of the child by being subject to an exemption safeguard mechanism under a structured exemption application process.* *(2) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child for such purposes as are specified in Part B of Fourth Schedule, subject to such conditions as are specified in the said Part, provided that such processing complies with the well-being of the child by being subject to an exemption safeguard mechanism under a structured exemption application process.*
(**Rule 12**)	*(1)A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is notified as such or is included in the class of Data Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the rules made thereunder.* *(2)A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit.* *(3)A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed by it for*	*(1) A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is notified as such or is included in the class of Data Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the rules made thereunder.* *(2)A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations further classified into high-risk, medium-risk, and low-risk observations based upon the potential threat or impact such observations bring to the objectives of these rules in the Data Protection Impact Assessment and audit.* *a. High-risk findings being those that pose*

	hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals. *(4)A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government on the basis of the recommendations of a committee constituted by it is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.*	*prompt and substantial threats to data privacy. Such findings shall be reported to the Board within 30 days of such findings with a proposed mitigation plan.* *b. Medium-risk findings being those which have been tracked to bring disturbance, and requires a corrective measure to be adopted in the near future are to be reported to the Board within 60 days of such finding with suggestive actions.* *c. Low-risk findings being those to be reported to the board and to be solved internally, or through the advice of the Board.* *The board shall be imposed with penalties in case of failure to resolve the threats identified through the observations.* *(3)A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data:* *a. undergoes various testing procedures to prevent unfair profiling, bias, discrimination, or any other practice negatively impacting data principles,* *b. is required to have independent audits at least once a year, along with a detailed report to be submitted to the Board.* *c.* *(4) A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government on the basis of the recommendations of a committee constituted by it is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.* *(5) If a Significant Data Fiduciary fails to perform his duty under sub-section (1) of sub-section (2) of this rule within the prescribed time, s/he shall be penalised with fine of 2% of*

		his/her annual turnover, or an amount prescribed by the Board, whichever is higher.
\ (**Rule 14**)	*Transfer to any country or territory outside India of personal data processed by a Data Fiduciary—* *(a) within the territory of India; or* *(b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India,* *is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.*	*Transfer to any country or territory outside India of personal data processed by a Data Fiduciary—* *(a) within the territory of India; or* *(b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India,* *is subject to the following conditions-* *(i) standard contractual clauses approved by Data Protection Board of India, or,* *(ii) binding corporate rules for multinational corporations, or,* *(iii) only if (i) and (ii) are not applicable in rare circumstances, transfer of personal data to a country or an international organisation shall take place subject to-* *(a) that the transfer is explicitly consented to after the subject has been informed the potential risks, or,* *(b) that the transfer is absolutely essential for the performance or conclusion of a contract, or,* *(c) the transfer is essential for public interest, or,* *(d) the transfer is essential for exercise of fundamental or legal rights* *making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.*
(**Rule 15**)	*The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.*	*The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if any data processor or data fiduciary processing the data has adhered to standards specified in the Second Schedule; and when,* *(1.) Identity of the data principal is disclosed but,*

		(i) consent given by the Data Principal is free, specific, informed, unconditional and unambiguous with a clear affirmative action, and signifies an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose, *(ii) the data principal is expressly informed if their personal data will be used for commercial or non-commercial purposes,* *(iii) the data principal has the right to withdraw their consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.* *(2) Or, when consent is not taken, the data is either anonymised or pseudonymised such that the privacy of data subjects is protected while valuable research can proceed.*
(Rule 16)	*1) The Central Government shall constitute a Search-cum-Selection Committee, with the Cabinet Secretary as the chairperson and the Secretaries to the Government of India in charge of the Department of Legal Affairs and the Ministry of Electronics and Information Technology and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as Chairperson.* *(2) The Central Government shall constitute a Search-cum-Selection Committee, with the Secretary to the Government of India in the Ministry of Electronics and Information Technology as the chairperson and the Secretary to the Government of India in charge of the Department of Legal Affairs, and two experts of repute having special*	*1) The Central Government shall constitute a Search-cum-Selection Committee, with the Cabinet Secretary as the chairperson and the Secretaries to the Government of India in charge of the Department of Legal Affairs and the Ministry of Electronics and Information Technology and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members with due consent of the Board, to recommend individuals for appointment as Chairperson. The prerequisites may vary as per the purpose of each such appointment, however must include area and years of policy experience and a compulsory background check.* *(2) The Central Government shall constitute a Search-cum-Selection Committee, with the Secretary to the Government of India in the Ministry of Electronics and Information*

	knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as a Member other than the Chairperson. *(3) The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee, appoint the Chairperson or other Member, as the case may be.* *(4) No act or proceeding of the Search-cum-Selection Committee specified in sub-rules (1) of this rule shall be called in question on the ground merely of the existence of any vacancy or absences in such committee or defect in its constitution.*	*Technology as the chairperson and the Secretary to the Government of India in charge of the Department of Legal Affairs, and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, subject to the approval of the Board, to recommend individuals for appointment as a Member other than the Chairperson.* *(3) The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee, appoint the Chairperson or other Member, as the case may be.* *(4) No act or proceeding of the Search-cum-Selection Committee specified in sub-rules (1) of this rule shall be called in question on the ground merely of the existence of any vacancy or absences in such committee or defect in its constitution.*
(Rule 19)	*Functioning of Board as digital office—The Board shall function as a digital office which, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual*	*Functioning of Board as digital office—The Board shall function as a digital office which, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual."* *"Provided that in cases where the Board is unable to function as a digital office due to infrastructural shortcomings or other unavoidable deficiencies, it may continue to function in a conventional manner until such deficiencies have been duly rectified* *Provided further, that such rectification shall be carried out within a period as decided by the central government for the purpose from the date on which the rules come into force."*
(**Rule 22**)	*(1) The Central Government may, for such purposes of the Act as are specified in*	*(1) The Central Government may, for such purposes of the Act as are specified in Seventh*

	Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, specify the time period within which the same shall be furnished and, where disclosure in this regard is likely to prejudicially affect the sovereignty and integrity of India or security of the State, require the Data Fiduciary or intermediary to not disclose the same except with the previous permission in writing of the authorised person. *(2) Provision of information called for under this rule shall be by way of fulfilment of obligation under section 36 of the Act.*	*Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, pursuant to a written order that specifies the legal basis for the request, the specific information required, and the reasons why such information is necessary and proportionate to achieve a legitimate purpose specified in the Seventh Schedule, specify the time period within which the same shall be furnished and, where disclosure in this regard is likely to prejudicially affect the sovereignty and integrity of India or security of the State, require the Data Fiduciary or intermediary to not disclose the same except with the previous permission in writing of the authorised person.* *(2) Provision of information called for under this rule shall be by way of fulfilment of obligation under section 36 of the Act* *(3) The person(s) against whom the data shall be informed of the action, through the Data Fiduciary or by any authorised agency. That the data collected by the authorised agency or agencies should be minimal, only pertaining to the case and as required which should not exceed a period of 60 days.* *(4) The period could be renewed upto a period of 180 days as granted by the High Court or Supreme Court with the individual being informed about the class of data collected and the period for which he was surveilled within a short period.* *(5) That after the expiration of the stipulated period, the data collected by the authorities be erased and not localised in due time.*
(**Schedule 1 and 2**)	*FIRST SCHEDULE* *PART A* ***Conditions of registration of Consent***	*. FIRST SCHEDULE* *PART A* ***Conditions of registration of Consent***

	Manager *1. The applicant is a company incorporated in India.* *2. The applicant has sufficient capacity, including technical, operational and financial capacity, to fulfil its obligations as a Consent Manager.* *3. The financial condition and the general character of management of the applicant are sound.* *4. The net worth of the applicant is not less than two crore rupees.* *5. The volume of business likely to be available to and the capital structure and earning prospects of the applicant are adequate.* *6. The directors, key managerial personnel and senior management of the applicant company are individuals with a general reputation and record of fairness and integrity.* *7. The memorandum of association and articles of association of the applicant company contain provisions requiring that the obligations under items 9 and 10 of Part B are adhered to, that policies and procedures are in place to ensure such adherence, and that such provisions may be amended only with the previous approval of the Board* *8. The operations proposed to be undertaken by the applicant are in the interests of Data Principals.* *9. It is independently certified that— (a) the interoperable platform of the applicant to enable the Data Principal to give, manage, review and withdraw her consent is consistent with such data protection standards and assurance framework as may be published by the Board on its website from time to time; and (b) appropriate technical and organisational measures are in place to ensure adherence to such standards and framework and effective*	***Manager*** *1. The applicant is a company incorporated in India.* *2. The applicant has sufficient capacity, including technical, operational and financial capacity, to fulfil its obligations as a Consent Manager.* *3. The financial condition and the general character of management of the applicant are sound.* *4. The net worth of the applicant is not less than two crore rupees.* *5. The volume of business likely to be available to and the capital structure and earning prospects of the applicant are adequate.* *6. The directors, key managerial personnel and senior management of the applicant company are individuals with a general reputation and record of fairness and integrity.* *7. The memorandum of association and articles of association of the applicant company contain provisions requiring that the obligations under items 9 and 10 of Part B are adhered to, that policies and procedures are in place to ensure such adherence, and that such provisions may be amended only with the previous approval of the Board* *8. The operations proposed to be undertaken by the applicant are in the interests of Data Principals.* *9. It is independently certified that— (a) the interoperable platform of the applicant to enable the Data Principal to give, manage, review and withdraw her consent is consistent with such data protection standards and assurance framework as may be published by the Board on its website from time to time; and (b) appropriate technical and organisational measures are in place to ensure adherence to such standards and framework and effective observance of the obligations under item 11 of Part B.* *10.The consent manager must provide expert*

	observance of the obligations under item 11 of Part B. *PART B* *Obligations of Consent Manager* *1. The Consent Manager shall enable a Data Principal using its platform to give consent to the processing of her personal data by a Data Fiduciary onboarded onto such platform either directly to such Data Fiduciary or through another Data Fiduciary onboarded onto such platform, who maintains such personal data with the consent of that Data Principal.* *Individuals are enabled to give, manage, review and withdraw their consent to the processing of their personal data through P, a platform maintained by a Consent Manager. X, an individual, is a registered user on P. B1 and B2 are banks onboarded onto P.* *Case 1: B1 sends a request on P to X for consent to process personal data contained in her bank account statement. X maintains the bank account statement as a digital record in her digital locker. X uses P to directly give her consent to B1, and proceeds to give B1 access to her bank account statement.* *Case 2: B1 sends a request on P to X for consent to process personal data contained in her bank account statement. X maintains her bank account with B2. X uses P to route her consent through B2 to B1, while also digitally instructing B2 to send her bank account statement to B1. B2 proceeds to send the bank account statement to B1.* *2. The Consent Manager shall ensure that the manner of making available the personal data or its sharing is such that the contents thereof are not readable by it.* *3. The Consent Manager shall maintain on*	*professional knowledge in data protection law and IT security, the scope depending on the complexity of data processing and the size of the company.* *PART B* *Obligations of Consent Manager* *1. The Consent Manager shall enable a Data Principal using its platform to give consent to the processing of her personal data by a Data Fiduciary onboarded onto such platform either directly to such Data Fiduciary or through another Data Fiduciary onboarded onto such platform, who maintains such personal data with the consent of that Data Principal.* *Individuals are enabled to give, manage, review and withdraw their consent to the processing of their personal data through P, a platform maintained by a Consent Manager. X, an individual, is a registered user on P. B1 and B2 are banks onboarded onto P.* *Case 1: B1 sends a request on P to X for consent to process personal data contained in her bank account statement. X maintains the bank account statement as a digital record in her digital locker. X uses P to directly give her consent to B1, and proceeds to give B1 access to her bank account statement.* *Case 2: B1 sends a request on P to X for consent to process personal data contained in her bank account statement. X maintains her bank account with B2. X uses P to route her consent through B2 to B1, while also digitally instructing B2 to send her bank account statement to B1. B2 proceeds to send the bank account statement to B1.* *2. The Consent Manager shall ensure that the manner of making available the personal data or its sharing is such that the contents thereof are not readable by it.* *3. The Consent Manager shall maintain on its platform a record of the following, namely:—*

	its platform a record of the following, namely:— (a) Consents given, denied or withdrawn by her; (b) Notices preceding or accompanying requests for consent; and (c) Sharing of her personal data with a transferee Data Fiduciary. *4. The Consent Manager— (a) shall give the Data Principal using such platform access to such record; (b) shall, on the request of the Data Principal and in accordance with its terms of service, make available to her the information contained in such record, in machine-readable form; and (c) shall maintain such record for at least seven years, or for such longer period as the Data Principal and Consent Manager may agree upon or as may be required by law.* *5. The Consent Manager shall develop and maintain a website or app, or both, as the primary means through which a Data Principal may access the services provided by the Consent Manager.* *6. The Consent Manager shall not sub-contract or assign the performance of any of its obligations under the Act and these rules.* *7. The Consent Manager shall take reasonable security safeguards to prevent personal data breach.* *8. The Consent Manager shall act in a fiduciary capacity in relation to the Data Principal.* *9. The Consent Manager shall avoid conflict of interest with Data Fiduciaries, including in respect of their promoters and key managerial personnel.* *10. The Consent Manager shall have in place measures to ensure that no conflict of interest arises on account of its directors, key managerial personnel and senior management holding a directorship, financial interest, employment or beneficial ownership in Data Fiduciaries, or having a material pecuniary relationship with them.* *11. The Consent Manager shall publish in an*	*(a) Consents given, denied or withdrawn by her; (b) Notices preceding or accompanying requests for consent; and (c) Sharing of her personal data with a transferee Data Fiduciary.* *4. The Consent Manager— (a) shall give the Data Principal using such platform access to such record; (b) shall, on the request of the Data Principal and in accordance with its terms of service, make available to her the information contained in such record, in machine-readable form; and (c) shall maintain such record for at least seven years, or for such longer period as the Data Principal and Consent Manager may agree upon or as may be required by law.* *5. The Consent Manager shall develop and maintain a website or app, or both, as the primary means through which a Data Principal may access the services provided by the Consent Manager.* *6. The Consent Manager shall not sub-contract or assign the performance of any of its obligations under the Act and these rules.* *7. The Consent Manager shall take reasonable security safeguards to prevent personal data breach.* *8. The Consent Manager shall act in a fiduciary capacity in relation to the Data Principal.* *9. The Consent Manager shall avoid conflict of interest with Data Fiduciaries, including in respect of their promoters and key managerial personnel.* *10. The Consent Manager shall have in place measures to ensure that no conflict of interest arises on account of its directors, key managerial personnel and senior management holding a directorship, financial interest, employment or beneficial ownership in Data Fiduciaries, or having a material pecuniary relationship with them.* *11. The Consent Manager shall publish in an easily accessible manner, on its website or app,*

	easily accessible manner, on its website or app, or both, as the case may be, information regarding— (a) the promoters, directors, key managerial personnel and senior management of the company registered as Consent Manager; (b) every person who holds shares in excess of two per cent of the shareholding of the company registered as Consent Manager; (c) every body corporate in whose shareholding any promoter, director, key managerial personnel or senior management of the Consent Manager holds shares in excess of two per cent. as on the first day of the preceding calendar month; and (d) such other information as the Board may direct the Consent Manager to disclose in the interests of transparency. *12. The Consent Manager shall have in place effective audit mechanisms to review, monitor, evaluate and report the outcome of such audit to the Board, periodically and on such other occasions as the Board may direct, in respect of— (a) technical and organisational controls, systems, procedures and safeguards; (b) continued fulfilment of the conditions of registration; and (c) adherence to its obligations under the Act and these rules.* *13. The control of the company registered as the Consent Manager shall not be transferred by way of sale, merger or otherwise, except with the previous approval of the Board and subject to fulfilment of such conditions as the Board may specify in this behalf.* *Note:* *In this Schedule,— (a) the expression "body corporate" shall include a company, a body corporate as defined under clause (11) of section 2 of the Companies Act, 2013 (18 of 2013), a firm, a financial institution, a scheduled bank or a public sector enterprise established or constituted by or under any Central Act, Provincial Act or State Act, and*	*or both, as the case may be, information regarding— (a) the promoters, directors, key managerial personnel and senior management of the company registered as Consent Manager; (b) every person who holds shares in excess of two per cent of the shareholding of the company registered as Consent Manager; (c) every body corporate in whose shareholding any promoter, director, key managerial personnel or senior management of the Consent Manager holds shares in excess of two per cent. as on the first day of the preceding calendar month; and (d) such other information as the Board may direct the Consent Manager to disclose in the interests of transparency.* *12. The Consent Manager shall have in place effective audit mechanisms to review, monitor, evaluate and report the outcome of such audit to the Board, periodically and on such other occasions as the Board may direct, in respect of— (a) technical and organisational controls, systems, procedures and safeguards; (b) continued fulfilment of the conditions of registration; and (c) adherence to its obligations under the Act and these rules.* *13. The control of the company registered as the Consent Manager shall not be transferred by way of sale, merger or otherwise, except with the previous approval of the Board and subject to fulfilment of such conditions as the Board may specify in this behalf.* *14. The Consent Manager shall act in a fiduciary capacity solely with respect to the performance of its regulatory duties and shall maintain complete operational independence from any data fiduciary or its subsidiaries.* *15. Sector-specific Consent Managers shall be appointed to ensure that oversight and compliance measures are tailored to the unique requirements of each industry handling personal data.* *Note:* *In this Schedule,— (a) the expression "body*

	any other incorporated association of persons or body of individuals; *(b) the expressions "company", "control", "director" and "key managerial personnel" shall have the same meanings as are respectively assigned to them in the Companies Act, 2013 (18 or 2013);* *(c) the expression "net worth" shall mean the aggregate value of total assets as reduced by the value of liabilities of the Consent Manager as appearing in its books of accounts; and (d) the expressions "promoter" and "senior management" shall have the same meanings as are respectively assigned to them in the Companies Act, 2013 (18 or 2013).* *SECOND SCHEDULE* *[See rules 5(2) and 15]* *Standards for processing of personal data by State and its instrumentalities under clause (b) of section 7 and for processing of personal data necessary for the purposes specified in clause (b) of sub-section (2) of section 17* *Implementation of appropriate technical and organisational measures to ensure effective observance of the following, in accordance with applicable law, for the processing of personal data, namely:—* *(a) Processing is carried out in a lawful manner; (b) Processing is done for the uses specified in clause (b) of section 7 of the Act or for the purposes specified in clause (b) of sub-section (2) of section 17 of the Act, as the case may be;* *(c) Processing is limited to such personal data as is necessary for such uses or achieving such purposes, as the case may be;* *(d) Processing is done while making reasonable efforts to ensure the accuracy of personal data; (e) Personal data is retained till required for such uses or achieving such*	*corporate" shall include a company, a body corporate as defined under clause (11) of section 2 of the Companies Act, 2013 (18 of 2013), a firm, a financial institution, a scheduled bank or a public sector enterprise established or constituted by or under any Central Act, Provincial Act or State Act, and any other incorporated association of persons or body of individuals;* *(b) the expressions "company", "control", "director" and "key managerial personnel" shall have the same meanings as are respectively assigned to them in the Companies Act, 2013 (18 or 2013);* *(c) the expression "net worth" shall mean the aggregate value of total assets as reduced by the value of liabilities of the Consent Manager as appearing in its books of accounts; and (d) the expressions "promoter" and "senior management" shall have the same meanings as are respectively assigned to them in the Companies Act, 2013 (18 or 2013).* *SECOND SCHEDULE* *[See rules 5(2) and 15]* *Standards for processing of personal data by State and its instrumentalities under clause (b) of section 7 and for processing of personal data necessary for the purposes specified in clause (b) of sub-section (2) of section 17* *Implementation of appropriate technical and organisational measures to ensure effective observance of the following, in accordance with applicable law, for the processing of personal data, namely:—* *(a) Processing is carried out in a lawful manner; (b) Processing is done for the uses specified in clause (b) of section 7 of the Act or for the purposes specified in clause (b) of sub-section (2) of section 17 of the Act, as the case may be;* *(c) Processing is limited to such personal data as is necessary for such uses or achieving such purposes, as the case may be;*

	purposes, as the case may be, or for compliance with any law for the time being in force; *(f) Reasonable security safeguards to prevent personal data breach to protect personal data in the possession or under control of the Data Fiduciary, including in respect of any processing undertaken by it or on its behalf by a Data Processor;* *(g) Where processing is to be done under clause (b) of section 7 of the Act, the same is undertaken while giving the Data Principal an intimation in respect of the same and—* *(i) giving the business contact information of a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data; (ii) specifying the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may exercise her rights under the Act; and (iii) is carried on in a manner consistent with such other standards as may be applicable to the processing of such personal data under policy issued by the Central Government or any law for the time being in force; and* *(h) Accountability of the person who alone or in conjunction with other persons determines the purpose and means of processing of personal data, for effective observance of these standards*	*(d) Processing is done while making reasonable efforts to ensure the accuracy of personal data; (e) Personal data is retained till required for such uses or achieving such purposes, as the case may be, or for compliance with any law for the time being in force;* *(f) Reasonable security safeguards to prevent personal data breach to protect personal data in the possession or under control of the Data Fiduciary, including in respect of any processing undertaken by it or on its behalf by a Data Processor;* *(g) Where processing is to be done under clause (b) of section 7 of the Act, the same is undertaken while giving the Data Principal an intimation in respect of the same and—* *(i) giving the business contact information of a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data; (ii) specifying the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may exercise her rights under the Act; and (iii) is carried on in a manner consistent with such other standards as may be applicable to the processing of such personal data under policy issued by the Central Government or any law for the time being in force; and* *(h) Accountability of the person who alone or in conjunction with other persons determines the purpose and means of processing of personal data, for effective observance of these standards.* *(i) For the purposes of these Rules, "instrumentalities" of the state shall mean governmental bodies, agencies, or any entity that is directly controlled by or established pursuant to statutory authority, excluding any private or commercial entities not explicitly designated*

		(j) Data processing by the State or its instrumentalities shall be strictly limited to the original purpose for which the personal data was collected, Any subsequent processing not directly related to the initial service for which consent was obtained shall require the explicit consent of the data principal. *(k) A mechanism shall be established for notifying data principals whenever their personal data is used for purposes other than those originally consented to.*
(**Schedule 3 and 4**).	*(1)Data Fiduciary who is an e-commerce entity having not less than two crore registered users in India* *For all purposes, except for the following:* *(a) Enabling the Data Principal to access his user account; and* *(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services* *Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest* *(2)Data Fiduciary who is an online gaming intermediary having not less than fifty lakh registered users in India* *For all purposes, except for the following:* *(a) Enabling the Data Principal to access his user account; and* *(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the*	*(1)Data Fiduciary who is an e-commerce entity having not less than one crore registered users in India* *For all purposes, except for the following:* *(a) Enabling the Data Principal to access his user account; and* *(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services* *Five years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest* *(2)Data Fiduciary who is an online gaming intermediary having not less than twenty-five lakh registered users in India* *For all purposes, except for the following:* *(a) Enabling the Data Principal to access his user account; and* *(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary,*

	digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services *Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest* *(3)Data Fiduciary who is a social media intermediary having not less than two crore registered users in India* *For all purposes, except for the following:* *(a) Enabling the Data Principal to access his user account; and* *(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services* ***Three years** from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest*	*and may be used to get money, goods or services* *Five years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest* *(3)Data Fiduciary who is a social media intermediary having not less than one crore registered users in India* *For all purposes, except for the following:* *(a) Enabling the Data Principal to access his user account; and* *(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services* ***Five years** from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest*

COMMENTS AND SUGGESTIONS ON THE DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

RULE 2 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025, R/w SECTION 2 OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

SECTION 2(I) OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

SUMMARY OF RECOMMENDATIONS

Section 2(i) of the DPDP Act, 2023 includes the definition of Data Fiduciary. It is suggested that this provision in a sub part should also include the Guardian Data Fiduciaries under its ambit. The general definition of Data Fiduciary is not sufficiently equipped to Data Fiduciaries which deal with large amounts of children data.

ANALYSIS

The definition of data fiduciary " means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data". While this definition brings all data fiduciaries dealing with personal data of adults (persons capable of giving consent) under its ambit, but it does not create a special category of data fiduciaries who deal with larger amounts of children data. A clear distinction needs to be drawn between children's data and consenting person's personal data. Such an inclusion in the definition fills a crucial gap in privacy protection at a time when children are increasingly going online and existing privacy laws aren't designed specifically to address children's vulnerabilities. Legislations such as Children's Online Privacy Protection Act[1] in the USA and previous iterations of PDP 18[2] and PDP 19[3] provided for separate class of data fiduciaries who were involved in operations and services regarding processing large volumes of children's data.

[1] Children's Online Privacy Protection Rule, Federal Trade Commission, 1998
[2] The Personal Data Protection Bill, 2018, Bill No. 373 of 2018, Lok Sabha, 16th Parl., 2018 (India).
[3] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Lok Sabha, 17th Parl., 2019 (India)

RECOMMENDATIONS

The suggested recommendations take into consideration the sensitive nature of children data and take learnings and insights from foreign legislations and previous drafts of the Personal Data Protection Bill of 2018 and 2019. This change is aimed at providing the data of children distinction from other personal data. It is also suggested that rules and guidelines may be released by the government which make provision for the data fiduciaries specifically dealing with large amounts of children data.

SECTION 2(x) OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

SUMMARY OF RECOMMENDATIONS

Section 2(x) of the DPDP Act, 2023 includes the definition of processing . It is suggested that this provision in a sub part should also include data consultation under its ambit. The definition of processing includes all possible types of data processing but does not include data consultation which is also an important avenue that should be included in the definition under Section 2(x) of the DPDP Act, 2023.

ANALYSIS

The existing definition of processing under Section 2(x) of the DPDP Act, 2023 is "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction. It is suggested to include data consultation under its ambit as data consultation means accessing stored information through targeted searches, such as using search routines to find and display data[4]. It is pertinent to note that the European Union's GDPR[5] includes consultation in its definition of processing. The inclusion of consultation as a form of processing within the larger definition of "processing" underscores GDPR's extensive approach towards data protection as it triggers data compliance requirements even

[4] The General Data Protection Regulation (GDPR) § 4 (2016).
[5] The General Data Protection Regulation (GDPR), The European Parliament and of the Council (2016)

at mere viewing of data. Including such provisions into the definition helps strengthen the data regulatory mechanism as even mere viewing of data invites regulatory scrutiny.

RECOMMENDATIONS

The suggested recommendation advocates for the inclusion of data consultation within the existing definition of data processing, this inclusion is suggested after thorough research of the GDPR. Data consultation is an important form of data processing, major consultancy companies in the world indulge in data consultancy. While such data consultancy companies do not sell or further process sensitive data but they use this data for advisory purposes while helping to make better decisions and help their clients and partner organizations with such data.

SECTION 2(z) OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

SUMMARY OF RECOMMENDATIONS

Section 2(z) of DPDP Act, 2023 includes the definition of Significant Data Fiduciaries. It is suggested that creating some objective pre decided criterias for the classification as Significant Data Fiduciaries. The present definition of Significant Data Fiduciaries gives a lot of autonomy regarding the designation of a Data Fiduciary as Significant Data Fiduciary.

ANALYSIS

The existing definition of the Significant Data Fiduciaries in Section 2(z) of DPDP Act, 2023 says "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10[6]. In the first reading this definition seems as if the government has the entire control to designate a Significant Data Fiduciary. However there are several criterias which are given in section 10 of DPDP Act, 2023. These are the criterias enlisted in section 10 of DPDP Act, 2023:

(a) the volume and sensitivity of personal data processed;

[6] The Digital Personal Data Protection Act, 2023, §10.

(b) risk to the rights of Data Principal;

(c) potential impact on the sovereignty and integrity of India;

(d) risk to electoral democracy;

(e) security of the State;

(f) public order.

The criterias/metrics which are presently there in the DPDP Act, 2023 are very open ended and arbitrary. It is suggested that some quantifiable criteria should be devised for the designation of Significant Data Fiduciary in addition to the power with the government under section 10. Parallels can be drawn from the definition of Systemically Significant Digital Enterprise in India's draft Digital Competition Bill, 2024[7] and definition of "Gatekeepers" in the European Union's Digital Markets Act, 2022[8] which have pre pre-decided criteria based on turnover and number of users . While these definitions are Competition Law centric, they can be used as a reference to make Data Privacy Centric Criterias.

RECOMMENDATIONS

These recommendations are aimed at reducing the governmental influence in the designation of Significant Data Fiduciary by the creation of objective criterions but still the final power rests with the government and they can designate Significant Data Fiduciary under section 10 of the DPDP Act, 2023. The creation of objective criterions will in turn help reduce the burden of the Government. Such objective quantifiable criterions will automatically designate such data fiduciaries who have crossed the pre decided threshold and if some data fiduciary which hasn't crossed the threshold but still is significantly important then the government under section 10 can designate them as Significant Data Fiduciary.

[7] MINISTRY OF CORP AFFAIRS, GOV'T OF IND., Report of the Committee on Digital Competition Law, 97 (2024).
[8] The Digital Markets Act, 2022

RULE 3 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Under Rule 3, Notices shall be industry specific to ensure relevance. One fits all approach may not be viable as different industries will have different needs. State approved templates for different industries can enhance compliance mechanisms. The different data processing notices shall ease the data protection integration into various sectors of the economy.

ANALYSIS

Though, the rules have emphasis on specific details, to take a step further sector based approach should be advised. A one fits all approach may not be viable as different sectors have different data processing protocols. This standardised approach may obstruct establishing a transparent data privacy ecosystem for relevant stakeholders. Data Protection compliance and data stakeholder's understanding shall improve through sector specific notices. Without proper oversight businesses might get away with lesser restriction and accountability to safeguard individuals' data. For instance, healthcare notices shall detail patients medical records and how it ought to be used. Whereas financial sector notices must specify transaction related data protection approaches.

RECOMMENDATIONS

The data processing notices for each sector must be specific to adapt to their respective needs. Requirements differ between different sectors which makes a standardised approach to notices inefficient. Notices can be approved by states to provide industry-specific templates. An industry focused notice framework ensures businesses meet practicality and transparency needs which creates more efficient compliance for stakeholders. It maintains understanding of their data protocols through relevant information. The approach can be adapted from the USA laws where different regulators require different sets of privacy notices. The Federal Trade Commission

requires financial institutions to comply with the Gramm-Leach-Bliley Act[9] to send data processing notices. On the other hand, the health sector mandates notices to comply with The Health Insurance and Probability Act.[10]

RULE 4 (2)(C) OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The key recommendation here is to insert an additional sub-clause of Rule 4(2)(c) to mandate a procedural period to review Consent Manager applications. Under the recommended sub-clause, the suggestion of a 60 days timeline aims to ensure procedural efficiency. It prevents indefinite delays as technological advancements are rapid and bureaucratic methods can make it worse. Hence , the 60 days timeline enhances transparency and reduces red tapism. It aligns with principles of natural justice, ensuring that Consent Managers can operate without unnecessary bureaucratic overhaul.

ANALYSIS

The issue with DPDP Rules up until now has been its long delays and uncertainty in establishing the rules. Such delays in future must be avoided at every step to ensure smooth progress. A 60-day timeline is recommended to improve operational efficiency by reducing needless delays which occur because of official procedures. This is because the existing red tapism in Indian bureaucracy may hinder compliance requirements. The fast tracked requirement enables Consent Managers application pass or reject quickly through a defined deadline. Which prevents it from getting caught up in lengthy regulatory procedures.

The GDPR guidelines specify certain time limits under Art. 64[11] on matters pertaining to the opinion of the board. It provides a minimum period of 8 weeks to conclude the board's opinion for multiple scenarios. Adapting a similar framework shall be in consonance with DPDPR being time efficient. While DPDPR provides a minimum

[9]The Gramm-Leach-Bliley Act, 1999.

[10] The Health Insurance and Probability Act, 1996.
[11] General Data Protection Regulation 2016, art. 64.

time limit of 6 months under Rule 18(9) to authenticate orders, a time limit for onboarding consent managers needs to be incorporated as well for administrative efficiency.

RECOMMENDATIONS

The recommended sub-clause of Rule 4 (2)(c) mandates a timeline approach that follows natural justice principles by establishing fairness and administrative transparency. The 60 days time frame promotes openness because stakeholders receive clear time limits to make decisions so they cannot face endless delays. The evolving technological environment may suffer if application processes exceed 60 days to an indefinite period. The reduction of bureaucratic obstacles enables more interested parties to become Consent Managers which strengthens both the competition and operational aspect of the system.

The 60-day timeline strikes the right balance between oversight regulations and operational efficiency which stops delays without sacrificing institutional accountability. A regimented period allows Consent Managers to connect easily with data governance programs and overcome procedural challenges thus delivering advantages to organizations and end users.

RULE 4 (4) OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Under Rule 4(4), a twelve month periodic review shall help the Consent Managers to remain updated with technology. This prevents obsolete compliance and regulations. Which further upholds data protection. It helps to maintain the effectiveness of consent manager's duties in protecting stakeholders rights amidst evolving digital ecosystems.

ANALYSIS

Technological development in the digital world means today's secure methods can easily become tomorrow's vulnerabilities. Regular updates are vital because out-of-date operations with redundant frameworks reduce the

rules ability to protect stakeholder rights. For example, the process of encryption standards keeps evolving. The encryption methods lose their relevance frequently since technology and means of cyberattacks keep updating. Hence, the stagnant security protocols of Consent Managers put user data at risk when they fail to conduct security updates.[12] India is the second most targeted nation when it comes to data theft instances. The total number of data theft incidents stood at 500 million in 2024 whereas this number is projected to grow over the next few years to 1 trillion.[13] Thus , the rule not having an obligation to mandate periodic evaluation of Consent Manager's duties may result in data protection lapses.

RECOMMENDATIONS

The suggestion for 4(4) is that there must be periodic evaluations every twelve months to maintain awareness about advancing technology. So consent managers can avoid using outdated compliance. The suggestion for 4(4) is that there must be periodic evaluations every twelve months to maintain awareness about advancing technology. So consent managers can avoid using outdated compliance

Such risks become manageable through regular reviews. Because they enable organisations to merge their practices with technology alongside regulatory needs. The Rules effectiveness together with transparency and security of consent management is preserved through these precautions. The proactive implementation of such adaptations by Consent Managers enables them to enhance data protection while sustaining user confidence in the continuously evolving digital network. A twelve month periodic review shall help the Consent Managers to remain updated with technology. This prevents obsolete compliance and regulations. Which further upholds data protection. Maintaining the effectiveness of consent manager's duties in protecting stakeholders rights amidst evolving digital ecosystems.

[12] "Encryption Security for a Post Quantum World" (*CSIS*, June 2, 2022) <https://www.csis.org/blogs/strategic-technologies-blog/encryption-security-post-quantum-world> accessed February 10, 2025

[13] Online E, "India Could Face 17 Trillion Cyberattacks by 2047: Report" *Economic Times* (October 30, 2024) <https://economictimes.indiatimes.com/news/india/india-could-face-17-trillion-cyberattacks-by-2047-report/articleshow/114771607.cms?from=mdr> accessed February 13, 2025

RULE 5 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Current Indian data governance frameworks, such as Schedule II of the Rules and the IT Act, 2008[14], permit state agencies to process personal data without fresh consent if users are informed, diverging from the Puttaswamy standard[15] requiring necessity, proportionality, and legitimacy for state privacy intrusions. Blanket authorisations under the IT Act enable broad data access without case-specific oversight, while undefined terms like "reasonable security safeguards" (Rule 6) and "instrumentalities" create ambiguity, undermining consent validity, data minimization, and accountability. To align with constitutional privacy principles, precise definitions of these terms are critical to enforce purpose limitation, clarify security obligations, and restrict overbroad interpretations that risk diluting safeguards. Instead of "instrumentalities", use of the term "public authorities" is recommended.

ANALYSIS

According to Schedule II of the Rules which governs standards for the processing of personal data by the state and its instrumentalities, the processing must meet several criteria, such as data being processed lawfully for the stated purposes and limited to the data necessary for achieving those purposes.[16] The Data Principals must also be informed about the processing and their means to access their rights.[17] Thus, state agencies can process data without fresh consent as long as users are informed, which deviates significantly from K.S Puttaswamy v. Union of India (2017)[18] which mandates that state interference with privacy must be necessary, legitimate and proportionate. Concerning modern legislations, These blanket authorisations have existed since the Information Technology Act, 2008, which dispenses with case-by-case authorizations for access to data in favour of blanket authorizations and permits the use of such data for broad and generic purposes.[19] Furthermore, there are still

[14] S Abraham and E Hickok, "Government Access to Private-Sector Data in India" (2012) 2 International Data Privacy Law 302, 305 <https://doi.org/10.1093/idpl/ips028>
[15] puttuswamy
[16] Ministry of Electronics and Information Technology, "Explanatory Note to Digital Personal Data Protection Rules, 2025" (2025) <https://www.meity.gov.in/writereaddata/files/Explanatory-Note-DPDP-Rules-2025.pdf>
[17] ibid.
[18] Justice K.S. Puttaswamy v. Union Of India, (2017) 10 SCC 1
[19] Rubinstein IS, Nojeim GT and Lee RD, "Systematic Government Access to Personal Data: A Comparative Analysis" (2014) 4 International Data Privacy Law 96 <https://academic.oup.com/idpl/article-abstract/4/2/96/734798?redirectedFrom=PDF>

ambiguities as to what "appropriate security safeguards" actually are, even with Rule 6 discussing reasonable security safeguards. This vagueness affects consent decisions and the rule's effectiveness as a whole due to the lack of clarity. Section 7 of the act which is mentioned uses the term "instrumentalities", which is again undefined and can lead to broad interpretations.

RECOMMENDATIONS

Due to terms such as "reasonable security safeguards" and "instrumentalities" being undefined and prone to broad interpretation, it is fair to request clear definitions or replacements of these terms to ensure the protection of personal data and to achieve the objectives of purpose limitation and data minimisation. Seeing as the term "reasonable security safeguards" finds mention in Rule 6 as well as clause (d) of the Second Schedule, they depend on circumstances which can include the nature of the entity processing the data as reasonable steps required would change based on its size, resources and complexity of operations, and amount of personal data held, as outlined in the Australian Privacy Principles guidelines.[20] The safeguards themselves may include training and managing employees in security program practices and procedures, assessing risks in information processing, and disposing of private information after it is no longer required by the Data Fiduciary, achieving the objective of purpose limitation.[21] The term "instrumentalities" can be replaced by the term "public authorities" which finds definition in Section 2(h) of the RTI Act, 2005.[22] The term "public authorities" is also used in the United Kingdom's Data Protection Act 2018.[23]

RULE 6 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Rule 6 aims to mandate data fiduciaries to operate reasonable security measures at technical and organisational levels. While the Rule is a step in the right direction, it still remains vague in certain aspects, such as "reasonable

[20] Oaic, "Chapter 11: APP 11 Security of Personal Information" (*OAIC*, October 12, 2023) para 11.7 <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information#taking-reasonable-steps>

[21] "SHIELD Act" (*New York State Attorney General*) <https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act>

[22] MINISTRY OF LAW AND JUSTICE, "THE RIGHT TO INFORMATION ACT, 2005" (2005) report s 2(h) <https://wcd.nic.in/sites/default/files/RTI%20ACT%20ENGLISH.pdf>

[23] King's Printer of Acts of Parliament, "Data Protection Act 2018" <https://www.legislation.gov.uk/ukpga/2018/12/section/7/enacted>

security safeguards" are not defined. The proposed recommendation under the newly introduced Rule 6 (1)(h) and Rule 6(3) is based on Article 32 of the GDPR[24] to specify certain benchmarks for technical measures. Moreover, along the same lines, the recommendation has also made a distinction between different levels of risk and sensitivity of data so that security measures are appropriate and proportionate. A six-months period has also been recommended to test and evaluate the security measures.

ANALYSIS

Rule 6 aims to provide reasonable security measures for data fiduciaries at technical and organisational levels. However, a clear distinction must be made between high and low risk and sensitivity data, as per which the measures must be proportionate and appropriate. This in in line with the aim of Article 32 of GDPR[25] where security measures are proportionate to the sensitivity of the data. Moreover, there must be regular cybersecurity audits every six months to test and evaluate the security measures. Additionally, minimum and reasonable security measures must be clearly defined and not be left in a vague manner open to interpretation.

RECOMMENDATIONS

The first recommendation is aimed at clearly distinguishing low and high risk and sensitivity data and that security measures must be appropriate and proportionate to the same. The second recommendation ensures that that regular cybersecurity audits are conducted to test and evaluate these security measures every six months. This is to ensure that these measures maintain compliance with the developing technology. Lastly, it is suggested that there is a clear definition to the "Minimum security measures" and "appropriate technical and organisational measures" to include but not limiting to encryption, pseudonymisation, ensure confidentiality and access control, obfuscation and masking. This is to ensure stronger legal enforcement and prevent data breaches.

[24] 'Art. 32 GDPR – Security of Processing' (General Data Protection Regulation (GDPR), 30 August 2016) <https://gdpr-info.eu/art-32-gdpr/> accessed 13 February 2025

[25] 'Art. 32 GDPR – Security of Processing' (General Data Protection Regulation (GDPR), 30 August 2016) <https://gdpr-info.eu/art-32-gdpr/> accessed 13 February 2025

RULE 7 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The amendment to Rule 7 as Rule 7 (c) seeks to further improve the accountability of the Data Fiduciaries. The key recommendations include setting 24 hours for notifying the Data Principal of a breach and requiring Data Fiduciaries to document all data breaches. This documentation must be made available to the board at any time to ensure compliance.

ANALYSIS

Rule 7 of the DPDP closely mirrors Articles 33[26] and 34[27] of the GDPR. It provides a mechanism to inform the Data Principal and the Board of any data breach. The key difference however is that it does not have any materiality threshold like GDPR. This change improves the accountability of the Data Fiduciaries who are obligated to report any kind of data breach, rather than arbitrarily deciding as to what constitutes a major data breach.

RECOMMENDATIONS

The first recommendation in this rule is creating a 24-hour time frame for reporting the data breach to the Data Principal. Although the rule states that the Data Principals must be notified without delay, it does not specify any timeframe for the same. Informing the Principals within 24 hours of the breach will further increase the accountability of the Data Fiduciaries.[28] The second recommendation is mandating that Data Fiduciaries document every data breach and make it available to the board whenever requested, similar to the provisions of Article 33(5) of the GDPR[29]. This will ensure the compliance of data fiduciaries to this rules.

[26] General Data Protection Regulation 2016, art. 33.

[27] General Data Protection Regulation 2016, art. 34.

[28] Kamesh Shekar and Vaishnavi Sharma, *Preliminary Analysis Draft Digital Personal Data Protection Rules, 2025,* The Dialogue (January, 2025).

[29] General Data Protection Regulation 2016, art. 33(5).

RULE 9 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The amendment to Rule 9 seeks to include specific contact information of the business, while also assigning a designated person to communicate with. Furthermore, it mandates the Data Fiduciary to display the relevant information on both website and app, if they are on both the platforms while also ensuring timely and accessible responses.

ANALYSIS

Although the original provision does not have any specific sections closely related to GDPR, Article 13 (1)(b)[30] talks about providing the contact information of the data protection officer. Article 12 of the GDPR[31] also puts emphasis on transparency and keeps the data controller in check. The amendment to the Rule provides better clarity to the concerned persons and also specifies the communication channels so that there can be no confusions and ensure that the responses are not delayed.

RECOMMENDATIONS

The first recommendation states that if a data fiduciary has both a website and an application in a mobile phone, the contact information should be displayed on both platforms. This makes it easily accessible for users to find the communication information regardless of the platform they are on, thus improving overall accessibility. The second recommendation emphasizes the need to offer several reliable channels of communication. This method caters to the needs of people trying to make contact and provides accessibility in case one means of communication is not available or breaks down. The third recommendation emphasizes the importance of having a specific person tasked with responding to questions on behalf of the data fiduciary. This creates definite accountability within the company and guarantees that questions are addressed by an authoritative body. The fourth recommendation requires that answers to questions should be given within a stipulated time frame and in

[30] GDPR art. 12, < https://gdpr-info.eu/art-12-gdpr/ >(last visited Feb. 17, 2025).
[31] GDPR art. 13, https://gdpr-info.eu/art-13-gdpr/ (last visited Feb. 17, 2025).

a reasonable manner. This enhances effectiveness in the process of communication and guarantees timely action taken on issues raised by individuals.

RULE 10 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The amendment to Rule 10 under the newly introduced Rule 10(2) seeks to include lawful guardians of children along with parents, whose consent must be sought before processing the data of a child. Further, mandating the Data Fiduciaries to create a mechanism to verify that the adult giving consent to the processing of the child is either a parent or a lawful guardian of the child.

ANALYSIS

Rule 10 of the DPDP Rules is created to work in coordination with Section 9 of the DPDP Act that provides for the processing of personal data of children. However, the rules only mandate the Data Fiduciaries to verify the age and identity of the person giving consent. It does not provide for a mechanism nor does it mandate the data fiduciaries to verify that the adults giving the consent for processing of children's data are actually the parents.

RECOMMENDATIONS

The first recommendation is allowing legal guardians of children to also permit processing of children's data in the absence of the parents.[32] The second recommendation is mandating the Data Fiduciaries to ensure that the person providing consent for the data processing of the child, is the parent of the child and the parent is identifiable.[33]

[32] Kamesh Shekar and Vaishnavi Sharma, *Preliminary Analysis Draft Digital Personal Data Protection Rules, 2025,* The Dialogue (January, 2025).
[33] Online Bureau, 'Is India's draft data protection rules enough to safeguard children's privacy?',*ET Legal World, (*6 January,2025), https://legal.economictimes.indiatimes.com/news/law-policy/is-indias-draft-data-protection-rules-enough-to-safeguard-childrens-privacy/116971400 accessed 12 February 2025.

RULE 11 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The proposed amendment to Rule 11 intends to provide more clarity with respect to the well-being of the child. It addresses the digital services as stipulated in the Fourth Schedule and proposes to add procedural safeguards. The exemptions need to be aligned with the interests of the child, and for that, blanket exemptions can be counter-productive to the intended purpose. This amendment seeks to establish an independent safeguard mechanism to protect the interests.

ANALYSIS

Rule 11 posits to be narrow and limited in its scope as it only includes data class fiduciaries under the Fourth Schedule, which includes educational institutions, daycare centers, healthcare professionals including mental health establishments. However, the scope remains narrow and vague as when considering 'well-being' of the child, a) that remains undefined under the DPDPA and b) the application of the rule is not well-structured as the question as to whether exemptions are applied in a blanket manner to those under the Schedule or whether there is a mechanism for it.

RECOMMENDATIONS

Due to the lack of transparency in how data fiduciaries can seek exemptions, the 'exemption safeguard mechanism' phrase aims to minimize the potential misuse that can be taken by data fiduciaries for processing personal data of children. There needs to be a defined exemption process to ensure compliance and establish parameters for application of this rule. Data fiduciaries who are engaged in the said classifications need to exemplify *how it* is necessary for their establishment to process children's data and whether the clinical professionals, allied healthcare workers or educational institutions require a complete exemption from processing children's data or whether it be a case specific instance. The extent of data collection should also be ensured, which comes under the purview of 'well-being.' This ensures that data is collected only for limited purposes, which gets approved by a set mechanism in place.

This exemption safeguard mechanism may function with a Review Board/Committee, in consonance with the Data Protection Board of India which will oversee the exemption requests. The exemption process will start with data fiduciaries applying for exemption, intended purpose, duration for the children's data usage. On acceptance of the application, the Board/Committee shall conduct periodic audits to ensure compliance with intended purpose and ensure no misuse of the data collected. The proposed amendment requires data fiduciaries to retain information for only the reasonable period as applied for, to fulfill a specific purpose for which it was collected. This provision explicitly states that operators cannot retain the information indefinitely. It is consistent with the US FTC's Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data[34] which was released in January 2025 and ensures transparency by public disclosure of applications and reporting additional information to FTC, similar which is proposed to be done to DPBI and the Review Board.

RULE 12 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Rule 12 of the Digital Personal Data Protection Rules imposes strict duties, responsibilities and compliances to a Significant Data Fiduciary in order to ensure data security, accountability, effective observance, and due diligence. For that very reason, there has been introduction to timely audits and Data Protection Impact Assessment under various subclauses and the newly introduced Rule 12 (5) which also ensures that the concerned board is up to date with its findings, suggestions, and recommendations. Such fiduciary responsibilities also include putting a check on emerging problems like keeping a check whether AI is harming any user, problems regarding confidential data sharing outside India, etc.

ANALYSIS

While the rule streamlines duties and responsibilities to ensure data privacy, it is broad and open to wide interpretation. Some phrases within the clauses require further clarification to ensure certainty rather than

[34] "FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data" (Federal Trade Commission, January 16, 2025) <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data>

ambiguity. The rule also addresses AI's growth, associated risks such as discriminatory practices and automated decision-making, but lacks provisions for checks on AI-generated results. There should be an addition of a provision requiring human review of AI-generated automated decisions in cases where fairness is in question.

Additionally, the provision aims to protect national interest and sovereignty but does not specify the extent of this protection. While such measures support national security by mitigating cyber spying, there is no clear indication of limits. Many Indian companies operate internationally and could be adversely affected by stringent yet vague laws on data sharing. Furthermore, the rule lacks provisions for penalizing non-compliance, which affects accountability and may lead to procedural delays. Rule 12 presents an opportunity to enhance data protection; however, its vague clauses, weak AI safeguards, and stringent yet ambiguous data-sharing regulations require refinement to prevent loopholes or harm to international businesses.

Clause 2 of Rule 12 does not define "significant observations," leaving room for broad interpretation. Observations could be categorized based on risk level and the necessity for resolution:

- **High-risk findings:** Those that pose immediate and substantial threats to data privacy should be reported to the Board within 30 days, along with a proposed mitigation plan.
- **Medium-risk findings:** Those that cause disruptions and require corrective action in the near future should be reported within 60 days, accompanied by suggested measures.
- **Low-risk findings:** These should be reported to the Board but can be resolved internally or with the Board's advice.

The Board should be subject to penalties if it fails to resolve identified threats.

Similarly, Clause 3 allows for wide interpretation and lacks clarity regarding due diligence. A clearer provision would provide specificity on how due diligence can be ensured and offer data fiduciaries a means to prevent liability in disputes by proving compliance with their responsibilities.

RECOMMENDATIONS

To address the concerns within Clause 3, the wording should be revised as follows:

(1) The data fiduciary shall observe due diligence to verify that the algorithmic software deployed for hosting, display, uploading, modification, publishing, transmission, storage, updating, or sharing of personal data:

Further, it is suggested that the data fiduciary undergoes various testing procedures to prevent unfair profiling, bias, discrimination, or any other practice negatively impacting data principles. Additionally, legislature must mandate independent audits at least once a year, with a detailed report submitted to the Board.

RULE 14 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Rule 14 aims to restrict transfer of data outside the national boundaries but fails to set clear procedures for the same. The recommendations provided aim to devise a clear-cut procedure for the transfer of data, thus not giving unbridled power to the Central Government. Transfer of data subject to standard contractual terms and binding corporate rules along with exceptions provided for rare circumstances is in line with the Chapter V of the General Data Protection Regulation.[35]

ANALYSIS

The aim of the proposed Rule 14 is to regulate the transfer of data outside of the national borders. However, for the purpose of regulation, it gives the Central Government unsupervised power. The recommendations aim for a more tierred approach to the transfer of data. The rule 14 closely aligns with Chapter V of the General Data Protection Regulation.[36] The Rule is powerful and empowers the government to restrict access to data. Additionally, in Rule 12(4) it has been mentioned that the Union government on the basis of the recommendations of a committee constituted by it can also determine the types of personal data that SDFs must localize within

[35] 'Chapter 5 – Transfers of Personal Data to Third Countries or International Organisations' (General Data Protection Regulation (GDPR), 5 October 2018) <https://gdpr-info.eu/chapter-5/> accessed 16 February 2025

[36] 'Chapter 5 – Transfers of Personal Data to Third Countries or International Organisations' (General Data Protection Regulation (GDPR), 5 October 2018) <https://gdpr-info.eu/chapter-5/> accessed 13 February 2025

India's borders. This grants the government significant power, with a broad scope of authority. The draft rules proposal to place restrictions on how Data Fiduciaries can share the data of Indian citizens with foreign governments is a positive step but foreign companies operating in India could find themselves in a difficult position and this rule can potentially lead to data localisation.[37]

RECOMMENDATIONS

The first recommendation is aimed at regulating the power of the government to control the access to data and prevent data localisation. By including Standard Contractual Terms and Binding Corporate Rules, which is in line with Article 46 of the GDPR, there is an introduction of a tiered system for transfer of data. [38] The second recommendation in the form of the proviso clause is aimed at to regulate the transfer in rare cases when the first two clauses are not applicable. This is in line with Article 49 of GDPR[39]. The recommendation is inspired from this provision which specifies the transfer of data in rare cases where it is subject to the explicit consent of the party, or to enforce contractual terms, or is for public interest, or to enforce fundamental or legal rights.

RULE 15 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The objective behind the amendment proposed under Rule 15 and addition of Rule 15(2) is that privacy of individuals and research progressions go hand in hand without hindering progress or infringing upon rights of privacy. This balance approach is based upon similar provisions contained in Article 89 of the GDPR[40]. Simultaneously, to avoid ambiguity as to who is required to follow the standards set in Schedule 2, it was seen essential to expressly make the addition of 'any data principal' to the provision.

---

[37] Rajmohan K, 'First Read on the Digital Personal Data Protection Rules 2025: Here's What You Need to Know' (Internet Freedom Foundation, 9 January 2025) <https://internetfreedom.in/first-read-on-the-dpdp-rules-2025/> accessed 13 February 2025

[38] 'GDPR, art. 46, Transfers Subject to Appropriate Safeguards' (General Data Protection Regulation (GDPR), 8 July 2020) < https://gdpr-info.eu/art-46-gdpr/ >

[39] 'Art. 49 GDPR – Derogations for Specific Situations' (General Data Protection Regulation (GDPR), 29 March 2018) < https://gdpr-info.eu/art-49-gdpr/ > accessed 13 February 2025

[40] General Data Protection Regulation 2016, art. 89.

ANALYSIS

Rule 15 of the DPDP Rules along with Section 17(2)(b) of the DPDP Act, 2023[41] provide an exemption from the application of the act when personal data is used for research, archiving or statistical purposes. Schedule 2 of the rules provides the standards which ought to be adhered to while using personal data for such purposes. While this exemption may ensure that innovation is not stifled through excessive regulations, the rule is riddled with certain ambiguities and require clarifications. The rules do not specify if consent will be obtained from the data principal before personal data is used for research, archiving or statistical purposes and if yes, the manner in which such consent can be given and withdrawn must also be expressly provided. While research activities have been exempted, research includes research for commercial purposes or is restricted to non-commercial research activities. If the former is the case, will this include personal data used in developing large language models since they would qualify as technological research? If it is the latter, there lacks clarity as to who will be permitted to make such use of data - any person or entity or will it be only those individuals/ entities whose primary purpose itself is research of if research is merely an ancillary to a prevailing commercial venture. Further, since Schedule 2 specifically states standards for the processing of personal data by the State and its instrumentalities, does this mean as per Rule 2, only the state may use personal data for research, archiving or statistical purposes.

RECOMMENDATIONS

The suggestions proposed to Rule 15 have been made keeping in mind the need to reduce ambiguity in the provision and also the scope for misuse. Furthermore, since the Apex Court has ruled that privacy is an absolute right when there is any scope for the identity of the data principal being revealed, then the element of obtaining consent and allowing the free withdrawal of such content is essential irrespective of the purpose for which the data is being processed. At the same time, India can also adopt the practice as provided in Article 89 of the General Data Protection Regulation (GDPR) according to which personal data can be processed for research purposes, without obtaining the data principal's consent but the processor ensures that the latter's privacy is not breached by keeping their identity completely anonymous at all times. For the same, the suggestions are as follows –

1. If there is even a slight chance that the identity of the data principal maybe revealed, then

[41] Digital Personal Data Protection Act 2023, s 17(2)(b).

a. Expressly mandate that the privacy of the data principals be taken before their personal data is processed,
b. Data Principals are made aware of the exact purpose for which their personal data shall be used and,
c. Data Principals have an option to withdraw their consent at any point in time and such an option must be easily exercisable as well.

2. And the alternate proposed is that the data principal is kept completely anonymous at all times.

In either circumstance, the data processors must work in accordance with the provisions of Schedule 2. However, since the schedule explicitly deals with standards to be followed by the state, we propose that the main provision of Rule 15 expressly states that ***Any*** data principal or data processor will have to adhere to these standards set in Schedule 2 of the DPDP Rules.

RULE 16 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The recommendations aim at providing certainty in the procedure for appointment of experts. There must be a transparent process for such appointments. Moreover, the appointment should be made ensuring that the independence of the Board is not affected.

ANALYSIS

Upon a bare reading of the rule, it is revealed that the excessive powers delegated to the government for the appointment of the Search-cum-selection committee may dilute the independence of the Data Protection Board of India. As mentioned in clause (1), the two experts are to be appointed as per the ‘opinion’ of the Central Government. The appointment also largely remains ambiguous, since there is no eligibility criteria mentioned. Moreover, the tenure of the experts is not mentioned.

RECOMMENDATIONS

For ensuring the independence of the Board and the appointment of competent individuals, the rules must provide for specific prerequisites tailored to the expertise for which they are being appointed. These prerequisites may include their area and years of policy experience and a compulsory background check. The Board must be made a party to such an appointment process and its opinion must be taken into consideration for the appointment of such experts. The tenure of the experts should be subject to the purpose of their appointment, and must be notified to the Board prior to their appointment.

RULE 19 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Rule 19 of the Draft Digital Personal Data Protection Rules, 2025 provides for a mandate for the Data Protection Board of India as a digital office. The intention behind the same is to enhance inclusivity and to reduce logistical barriers that hinder the functioning of the Board. While the Digital Personal Data Protection Act, 2023 already provides for the functioning of the Board as a digital office, the Rule enforces the same as an obligation. This transition comes with multiple challenges particularly accessibility, data security and technological limitations among the others. In order to tackle these key recommendations as elucidated upon in detail include capacity building and training programmes, increased awareness especially among marginalized sections, upgradation of digital infrastructure, robust security measures and the like. Overall, till a requisite situation is achieved, it is suitable for the Board as a hybrid model, combining both digital and physical participation. This is suggested to ease the process of transition and ensure success to foster a progressive and accessible framework that promotes justice, equity and inclusivity.

ANALYSIS

Rule 19 promotes the idea of modernization of the Data Protection Board of India. The same idea is already a part of the Digital Personal Data Protection Act, 2023 in the form of Section 28 of the Act[42] which provides that "The Board shall function as an independent body and shall, as far as practicable, function as a digital office". Though the Act provides the idea, it does not materialize it to be an obligation. The wording of Rule 19 reads

[42] Digital Personal Data Protection Act, 2023, § 28, No. 22, Acts of Parliament, 2023 (India).

“The Board shall function as a digital office”, thus making it an obligation for the Board to function as a digital office.

By mandating the functioning of the Board as digital, the draft rule proposes to eliminate the logistical barriers which are usually attached to the idea of physical presence of the Data Principal or the Data Fiduciary. These may include constraints associated with cost and time. Thus, this mandate shall facilitate increased and effective participation from parties and other stakeholders. Moreover, this adds an element of inclusivity in the functioning of the Board by allowing the relevant stakeholders to overcome the mobility impairments, thereby helping to foster a just and equitable legal process.

It is however pertinent to note that this transition to a completely digital framework shall come with multiple challenges. One of the most important concerns of the same shall be accessibility. Accessibility of virtual platforms, for the marginalized communities, due to lack of requisite resources and technical expertise may pose a great challenge to participation. And this lack of effective participation will eventually undermine the principle of fairness. This becomes even more important when the aspect of ‘lack of awareness’ is read with the same. Further, the primary idea behind introduction of digital office is to reduce logistical barriers but an alternate perspective of this rule will reveal its own set of logistical difficulties. These include technological limitations like internet connection and platform incompatibilities which can prove to be great inefficiencies to the procedure.

Data Security can also be a significant issue that the Rule may pose for the simple reason that an over-reliance on this digital idea can expose sensitive information to unauthorized access, misuse and a potential breach. This means that, to effectively bring the rule into force, strong security measures are required along with specific guidelines for ensuring that the integrity of the functioning of the Board is not compromised. Adequate safeguards need to be provided for the same in order to avoid the procedural impairment from affecting the success of the proposed rule.

The proposed rule is illustrative of progression but a mere mandate on the same as opposed to the possibility as provided by the Act might not be enough. Before the rule can be enforced, it is important to reconsider multiple details as aforementioned so as to ensure the success of the intended goal. Mitigating the risks associated with the digital world shall be the prime concern along with other concerns like accessibility.

RECOMMENDATIONS

As provided in the analysis, to ensure that the goal of the proposed rule is achieved, it is important to address the possible problems associated with the same. Firstly, the aspect of accessibility should be given prime importance. Before this can be ensured, awareness needs to be increased with special focus on the marginalized sections of the society. Methods that may be used for the same include capacity building programmes, training programmes, helplines. Post achievement of this basic level of awareness, the Board shall emphasize on the adoption of user-friendly virtual platforms that are easy for everyone to access and use.

Secondly, to tackle the problem of data security, measures like end-to-end encryption, multi-factor authentication, and secure login protocols and others should be made compulsory. Also, as mentioned earlier, a clear set of guidelines shall be laid down including penalties for the breach of these guidelines. Additionally, anonymization protocols, that are guidelines and practices that define how to de-identify data to protect privacy and use of proxy servers should be promoted to protect the participant's data.

Thirdly, to be able to deal with logistical difficulties the Board should evaluate and upgrade the digital infrastructure periodically. Alternate communication channels should be identified to be able to manage platform failures. Additionally, there should be effective testing of virtual proceedings before the enforcement can be effectively ensured.

Fourthly, since establishing a completely digital framework poses multiple challenges which might not be as easy to combat given the digital infrastructure situation currently, it shall be better to promote the functioning of the Board as per a hybrid model till the time there are enough resources available to go completely digital. This means combining digital and physical participation of the relevant stakeholders.

Lastly, since the Board has direct interaction with the public, it shall be better to invite regular feedback from stakeholders to be able to ensure fairness and effectiveness that draft is intending to introduce. The aforementioned recommendations are primarily focused on suggesting how the transition of the Board to a digital office be made smoother and to minimize the risk associated with the same. Adaptive procedures and consistent surveillance will guarantee that the digital framework complies with the values of justice, equity, and accessibility.

RULE 22 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

SUMMARY OF RECOMMENDATIONS

Rule No. 22, herewith Schedule 7, of the Digital Personal Data Protection Rules (2025) is directed towards the Data Fiduciaries to supply the authorised government agencies with data requested or ordered to be provided to the latter in a stipulated period of time which is subjected to the sort of data requested, kind of Data Principal(s) or sort of Data Fiduciary. The objectives behind the proposed amendments including addition of Rule 22(3), Rule 22(4) and Rule 22(5) are firstly, to provide a definitive idea and clear out ambiguity on how the requisition should be made by the Government Agency to the Fiduciary and that there's no arbitrary procedure pursued by the agencies acting. Secondly, to uphold the Right to Privacy as held in the case of *KS Puttaswamy v. Union of India (2017)* and also to keep the rules drafted to be in line with the *The Group of Experts on Privacy Issue* chaired by Justice AP Shah, The outcome being known as the *AP Shah Report of 2012* [43]and Legislations around the world as mentioned such as the *ALRC Report of 2008: For your Information* of Australia

ANALYSIS

It must be specified and demarcated as to what sort of data could come under purview and surveillance of The State and not merely mention the necessity of the state's sovereignty or compliance with the laws or audit which leaves a wider jurisdiction for the government agencies that can be misused.

Procedure:

There's lack of procedural directions stated therewith which makes it vague how the data can be requisite for the "audit" on whether the Fiduciary should be classified as a "Significant Data Fiduciary" and not mentioning the mode of requisition again leaves a grey area. Hence, it is favourable that the direction to the Fiduciary for the requisition of data be made in writing, in black and white for an unambiguous understanding on the part of both the Data Fiduciary and in future, the Data Principal, if allowed to.

[43] The Planning Commission, Justice AP Shah, Report of the Group of Experts on Privacy, The Centre for Internet and Society, < https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf >.

This lack of procedural fairness could be seen as a violation of *Puttaswamy Judgement* which called for the same and a three-pronged test which is that there should be:

- Legality of the law to permit such an intervention by the State
- The legitimate aim should be underscored.
- The means adopted to collect the data should be proportionate to the reason why it is being followed so.

By providing a document to the surveilled individual, at least electronically, and erasing the data collected, it will be dutiful of the government to do so and will make the government accountable and honest to its citizens. By not performing such duties, the jurisdiction will be of no boundaries and will be the breaching of fundamental rights of Right to Privacy as neither was consent asked for and nor was it known what type of data was even collected. This will also be a question mark on the citizen's Right to Life (with dignity and not with paranoia) and Right to Justice as the individual could have a copy for the basis of an appeal which he may make.

Retention of Data:

The AP Shah report makes this observation regarding corporate bodies:

> *The Body Corporate holding sensitive personal data will not retain that information for longer than is required for the purposes for which the information may be lawfully used or is required under any other law in force. Rule 5(4)*[44]

It should be considered that the Government should be accountable proportionately by not retaining the data collected under Rule 22 of the DPDP Rules (2025) and Schedule 7, herewith, conditioned to the "sovereignty, security and integrity" of the state which should be made specified in writing.

[44] Report of the Group of Experts on Privacy, ITA Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011, Rule 5(4) .

RECOMMENDATIONS

The recommendations have been made keeping in view that there lie lacuna and gaps that are to be defined and clarified for due compliance with the judgements upholding fundamental right of Privacy. It is believed that there should be at least some sort of a concession that is to be allowed to the individuals in the said regard. By keeping these checks and balances in place and making sure that the DPDP Rules of 2025 are consistent with the law.

This can ensured if the procedure of providing a furnished copy stating the class of data acquired by the Government Agency and the stipulated period of surveillance is provided to the individual before, during or even after the surveillance and the individual being informed that the surveillance has been extended for a specified period of time[45] (180 days) not arbitrarily.

That only useful information, pertaining to the case per se, should be collected and if there's anything more to be collected, there should be a record of it. The information should be retained for a certain period of time and must duly be erased as being accountable and being honest and trustworthy to citizens.

SCHEDULE 1 AND SCHEDULE 2 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The recommendations emphasize the need for **sector-specific consent managers** with clearly defined roles, independent from data fiduciaries, and subject to stricter qualification standards. Incentives should be introduced for data fiduciaries to comply, similar to Singapore's PDPA. Additionally, the definition of **"instrumentalities" of the state** must be clarified, and Section 7 refined to prevent misinterpretation. Data processing should strictly align with its original purpose, requiring **explicit consent** for further use, along with **clear standards for**

[45] Planning Commission, Group of Experts on Privacy Submit Report, Press Information Bureau < https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503 > .

"legitimate use." Data principals should be notified if their data is used beyond its original purpose, and **judicial oversight** must be mandated to ensure government accountability in data usage.

ANALYSIS

First Schedule:

The First Schedule of the Digital Personal Data Protection Rules, 2025 outlines the conditions for registering as a Consent Manager and their obligations. The rules outline registration conditions and obligations but *lack clarity scope of consent managers*, including their incentive to operate. It is unclear if a single consent manager will handle all personal data across all sectors or whether there will be sector-specific consent managers. Because there should be mandates with higher standards of data protection for sectors which handle sensitive information such as the medical sector.

The rules also suggest that data fiduciaries should be on boarded onto consent manager platforms. This may create issues as consent managers *will be responsible* for onboarding data fiduciaries. However, data fiduciaries might not be motivated to onboard unless *incentivized*, especially if they are already meeting their obligations under the Act. So taking from the Singapore's PDPA, their model for incentivizing compliance by mandating lower fines for companies that comply, are prime example of how we can move forward.[46]

Consent managers must act in a fiduciary capacity and *avoid conflicts of interest with data fiduciaries*.[47] The broad restrictions could prohibit data fiduciaries and their group entities from acting as consent managers for data processed in the same entity. This means that a company that acts as a data fiduciary might not be able to also be a consent manager for its own data processing or for data processed by a related company within the same group. It is unclear whether the conflict of interest restrictions apply only to data fiduciaries being onboarded by the

[46] Chong Kin Lim, Singapore - Data Protection Overview, Data Guidance(2024) [https://www.dataguidance.com/notes/singapore-data-protection-overview].
[47] Nick Lauw, Pu Fang Ching, Fines for PDPA Breaches: How Clear is the Crystal Ball?, RPCLegal (November, 2023) [https://www.rpclegal.com/thinking/data-and-privacy/fines-for-pdpa-breaches-how-clear-is-the-crystal-ball/]

consent manager, or if it extends to all data fiduciaries. This ambiguity raises concerns that *companies might need to engage external and unrelated consent managers, which can have the unintended consequences of adding layers of complexity, cost, and inefficiency* into the consent management ecosystem. This might harm innovation especially among the medium and small entities who may not have the capacity to afford an external consent manager.

There should also be a stricter standard in choosing of a consent manager, and rather than the vague “sufficient technical capacity” given in the rules, there is a necessity for stricter standards for qualification as a consent manager such as in EU’s GDPR , their qualification of choosing Data protection officers require the said officers to have expert knowledge about data protection law and practices.

Second Schedule:

The Second Schedule establishes minimum standards for data processing by the State and its instrumentalities for purposes exempted under the Act, such as providing subsidies, benefits, services, certificates, licenses, or permit. The rules specifically address exemptions for the state and its instrumentalities. There is a concern that data collected under other provisions, like “Certain Legitimate Uses,” could be used by the government without restrictions. The definition of "instrumentalities" remains ambiguous, which could lead to broad interpretations. For example could instrumentalities of the government mean, should it be limited to just official government agencies or could be stretched to PSE’s and to government contractors.

While the intention behind these provisions seems legitimate, it is unclear what specific circumstances necessitate data processing beyond the stated purposes. It is unclear what happens if other laws, such as those related to criminal investigations, require data; consent would not be needed under the exemptions, and there are no mandated standards for the State or its "instrumentalities". It also mandates that Data Principals be informed about the processing of their data by the State or its instrumentalities.

However, if a Data Principal has previously consented to a State service, the State can process that data for other unrelated services. There is a lack of explicit requirements to ensure that subsequent processing by the State is closely linked to the original service for which consent was given.[48]

Also, there is the ambiguity in regards to "legitimate uses" mentioned in the schedule, there is a lack clarity in which what legitimate use means, this lack of standards might to lead perversion of the legislative intent behind the act, it could become a loophole that allows the government to the need for consent in a variety of situation. We could take suggestions from Canada's Privacy Act , this act prohibits collection of data unless its directly related to a programme or activity by the govt. Under this act collection of data, that data should only be used for the purpose for in which it was collected and when needed to be used for something else fresh consent must be taken from the source of data (section 8), but the act also list out exceptions in this case, for needs of national security, law and order etc.

RECOMMENDATIONS

First Schedule:

It is suggested that to remove uncertainity regarding the role of consent managers and to promote a lawful data protection framework, legislature should provide explicit guidelines on the precise roles and responsibilities of consent managers. It is suggested that A Consent Manager shall have clearly defined responsibilities, including but not limited to monitoring data processing activities, verifying adherence to data protection standards, and ensuring that data fiduciaries comply with the obligations imposed herein. Further, the legislature must mandate sector-specific consent managers to ensure specialized oversight and compliance within each industry rather than a single entity managing all personal data across sectors. Fixing the statute on its essentials, further the legislature should mandate stricter qualifications for qualification as a consent manager, to provide for a more robust data protection framework.

Second Schedule:

It is suggested that to prevent unintended use of the Act by parties which should use it in compliance with law, legislature should provide a clear definition of "instrumentalities" of the state and refine the vague sub-sections

[48] Privacy Act, R.S.C. 1985, c. P-21 (Can.)

of Section 7 to limit potential misinterpretations. Secondly, it must clarify on the specific circumstances under which data can be processed, ensuring that it aligns with the original purpose of data collection. Thirdly, it must mandate explicit consent for any subsequent processing not directly related to the original service. Further to foster a more inclusive framework where all stakeholders have right to be informed of the use of data owned or stored by them, there should be a process for data principals to be notified of the use of their data if it is used for purposes other than the ones originally consented to.

SCHEDULE 3 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

Schedule 3 of the Draft digital Personal Data Protection rules, 2025 deals with time period for data retention by data fiduciaries falling under Rule 8(1) of the rules. The rules prescribe a 3 year period for data retention for data fiduciaries , passing of which, data must be erased. The schedule also prescribes certain user thresholds for such intermediaries, and it is suggested that these thresholds require a revision, considering that these thresholds are high and might allow smaller yet significant data holding enterprises to escape compliance under the act. Additionally, there is a suggestion to increase the time limit for data retention so as to ensure availability of data for regulatory audits, compliance and consumer disputes.

ANALYSIS

Schedule 3 of the Draft Digital Personal Data Protection Rules, 2025, establishes user thresholds and data retention periods for e-commerce, online gaming, and social media intermediaries. These provisions aim to regulate large-scale data fiduciaries, ensuring they retain user data responsibly and comply with privacy norms. It is suggested that under schedule 3, User thresholds are high which might allow enterprises possessing significant amounts of data to escape compliance under the act. Secondly, it is observed that the retention period of three years may not be adequate, particularly for sectors like e-commerce, social media, and gaming, where users frequently re-engage after extended periods. Many e-commerce businesses allow users to return and access purchase histories even after long gaps. Similarly, social media platforms retain personal data for personalized content recommendations, account recovery, and compliance with potential legal requests. Thirdly, the schedule

employs a one size fits all approach to the data retention compliance for such intermediaries. Considering the difference of use, availability and nature of data differing across multiple sectors, its imperative that the schedule creates even more distinction which industry specific to compliance with sensitive data needs of the industry.

RECOMMENDATIONS

1. Reducing User Thresholds for E-Commerce, Social Media, and Online Gaming Intermediaries

Under the first recommendation, it is suggested that E-commerce and social media intermediaries thresholds under the schedule be revised from **two crore users (20 million)** to **one crore users (10 million)** and Online gaming intermediaries thresholds be revised from **fifty lakh users (5 million)** to **twenty-five lakh users (2.5 million)**.

The current threshold of 2 crore users for social media and e-commerce intermediaries is significantly high and may allow several fast-growing platforms to operate without sufficient regulatory oversight. Lowering the threshold will bring more platforms under scrutiny and ensure compliance at an earlier stage of their growth. For Example: in India, platforms like Koo (an alternative to Twitter) and ShareChat (a regional social media platform) had fewer than 20 million users initially but grew exponentially. By the time they reached regulatory thresholds, potential data protection concerns had already arisen. Similarly, many e-commerce startups that handle vast amounts of personal and financial data remain outside compliance requirements until they reach the user threshold.

Comparing across foreign jurisdictions, it is suggested that inspiration be taken from EU General Data Protection Regulation[49]. Unlike India's threshold-based approach, GDPR applies to all entities processing EU citizens' data, regardless of size, emphasizing that data protection should be based on the nature of data processing rather than just user volume. Another example is the California Consumer Privacy Act (CCPA)[50] it applies to businesses that meet any one of three criteria, including annual gross revenue over $25 million, processing 50,000 or more consumer records annually, or deriving at least 50% of revenue from selling personal data. This is a much lower threshold than India's current limit and even in very inclusive comparatively.

[49] General Data Protection Regulation (GDPR) – Legal Text" (*General Data Protection Regulation (GDPR)*, < https://gdpr-info.eu/ >.
[50] "California Consumer Privacy Act (CCPA), *State of California - Department of Justice - Office of the Attorney General*, 2018 < https://oag.ca.gov/privacy/ccpa >.

Considering special nature of online gaming, online gaming platforms collect vast amounts of personal, behavioral, and financial data, including real-time location, payment details, and player habits.Lowering the threshold to 2.5 million users ensures that mid-sized gaming platforms implement security and compliance measures before they scale to larger audiences. Example: China's Data Protection Laws for Online Gaming[51] enforce strict regulations regardless of platform size, particularly for protecting minors from excessive gaming and data exploitation.

2. Increasing Data Retention Period to Five Years

Under the second recommendation, it is suggested to extend the **data retention period** from **three years** to **five years** across regulated platforms. Long-Term Compliance and Legal Necessity : Financial transactions, contractual obligations, and legal disputes often require access to older data. Additionally, a 3-year retention period is insufficient for many fraud investigations, regulatory audits, and consumer disputes. To that extent, an example of India's SEBI regulations mandate brokers to retain client records for seven years to comply with securities fraud investigations.

The data in the table given below provides data across multiple jurisdictions, suggesting different data retention periods for different industry specific needs, which is also currently more than as suggested in the 3rd Schedule.

Global Benchmarking on Data Retention:

Jurisdiction	Data Retention Period	Applicable Sector
United States (SEC & FINRA Regulations)[52]	5–7 years	Financial transactions, brokerage data

[51] Data Protection Laws in China - Data Protection Laws of the World, DLAPiper Data Protection, < https://www.dlapiperdataprotection.com/index.html?c=CN&t=law >.
[52] "SEC.Gov | Self-Regulatory Organization Rulemaking" < https://www.sec.gov/rules-regulations/self-regulatory-organization-rulemaking/finra >.

European Union (GDPR exceptions)[53]	5–10 years	Banking, law enforcement, tax compliance
Singapore (PDPA regulations)[54]	5 years minimum	Financial and corporate transactions
India (Income Tax Act)[55]	6 years	Tax and financial records

Fraud and cybercrime investigations often require access to older transaction data. Financial frauds, money laundering, and Ponzi schemes operate over extended timeframes, making a longer data retention policy essential. Additionally, GDPR and other data protection frameworks emphasize data minimization, ensuring data is not retained beyond its necessity. However, sectoral exemptions exist for financial, medical, and law enforcement data, balancing privacy with compliance needs. Hence, it is suggested to accommodate larger time frames for data retention.

3. Sector-Specific Adjustments for Data Retention Policies

The third recommendation suggests to introduce **sector-specific retention periods** instead of a **one-size-fits-all** approach. The table given below draws a comparison between India's current framework and best international practices:

[53] "Data Protection under GDPR - Your Europe" (*Your Europe*, January 1, 2022) <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm>.
[54] "PDPC | PDPA Overview" <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act >.
[55] Income Tax Act as amended by Finance (No. 2) Act, No. 43 of 1961, INDIA CODE (2023) < https://incometaxindia.gov.in/pages/acts/income-tax-act.aspx >.

Industry-Specific Data Retention Requirements

Sector	Current Retention Norms (India & Global)	Recommended Change
Financial Transactions	SEBI: 7 years (India), FCA: 5 years (UK), SEC: 7 years (U.S.)	Align with global best practices, minimum 5 years
Medical Records	India: 3 years, UK NHS: Lifetime for GP records	Increase to 7+ years for critical patient history
Cybercrime & Law Enforcement Data	No clear mandatory retention for digital evidence	Establish 5+ years for digital forensic evidence

It is suggested that one of the shortcomings of a uniform retention period is ignorance of operational realties and dynamic nature of different industries and sectors. For example, In financial fraud cases, fraudsters often manipulate data trails over extended periods, making a 3-year record limit impractical. Another good example in context of this elaboration is The Cambridge Analytica scandal [56], which demonstrated how personal data, even after years of retention, could be misused for political manipulation. So the regulatory lessons from the scandal

[56] Emma Graham-Harrison and Carole Cadwalladr, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach" *The Guardian* (September 29, 2021)
< https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election >.

highlight the need for stricter retention policies in high-risk sectors (e.g., social media & data analytics) while allowing controlled retention in finance and healthcare. Additionally, while accomodating this suggestion, vigilance and additional safeguards must be implemented. Hence, while extending retention periods, regulatory frameworks should mandate periodic security audits to prevent data breaches. For Example: Singapore's Cyber Security Act (2018) [57]requires periodic security reviews for retained financial and healthcare data.

SCHEDULE 7 OF THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

SUMMARY OF RECOMMENDATIONS

The aforementioned suggestions aim at preventing misuse via the overly broad language used in the text, emphasising upon usage of clear boundaries for both private and government use. The lack of independent oversight and clear guidelines governing the retention of data may increase the risk of unchecked data collection and indefinite storage. Basically, stricter safeguards and use of narrowly defined language has been emphasised.

ANALYSIS

Section 15, which talks about specific exemptions from restricting the processing of personal data for the sake of for the sake of research , archiving or statistical purposes given that it adheres to the specific standards outlined in Schedule II. However, the provision is overly broad and lacks clarity, leaving room for ambiguity. It fails to specify whether exemptions apply exclusively to government research bodies or if private entities may also invoke them. Allowing private players to use this legislation would likely create opportunities for exploitation, i.e. companies using the said data for profit driven research. Hence, lines need to be drawn on when and how private players as well as government agencies have the discretion to apply this rule.

Schedule 7 outlines the state's authority to process personal data under specific circumstances, it provides exemptions for government bodies allowing them to process personal data under certain conditions. Some key concerns with this piece of text can be related to the overly broad exemptions that allow extensive discretion of the government, which highlights the potential for misuse of the same. Also since we are talking about the government, there shall be an independent body to oversee the process and mechanisms to curb the scope of

[57] Cybersecurity Act" (*Cyber Security Agency of Singapore*) < https://www.csa.gov.sg/faqs/cybersecurity-act >.

misuse. In addition to this, there are no specific guidelines on how long the government can retain personal data, raising concerns about indefinite storage.

RECOMMENDATIONS

The law should clearly state whether exemptions apply only to government bodies or if private companies can also use them. If private players are included, strict conditions must prevent misuse for profit-driven research. It is further suggested that an independent body should oversee data use, ensuring risk assessments are conducted before processing. Clear data retention limits must be set to prevent indefinite storage. The overly broad exceptions allowing extensive discretion of the government shall be fixed and narrowed down further to prevent misuse.