Response by the Centre for Information Policy Leadership to the Ministry of Electronics and Information Technology's Notification of Draft Digital Personal Data Protection Rules 2025

Submitted March 4, 2025

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Notification issued on January 3, 2025, by India's Ministry of Electronics and Information Technology (MeitY) regarding the Draft Digital Personal Data Protection Rules 2025 ("Rules").

We have displayed our comments addressing the following Rules in the table that follows:

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

MeitY DRAFT TEXT	COMMENTS
RULE 1	
Rule 1.Short title and commencement. (1) These rules may be called the Digital Personal Data Protection Rules, 2025. (2) Rules 3 to 15, rule 21 and rule 22 shall come into force with effect from _____. (3) These rules, except rules 3 to 15 and rules 21 and 22, shall come into force on the date of their publication in the Official Gazette.	The Rules as a whole introduce a series of new operational and technical requirements. Given the complexities involved, especially for smaller businesses who will need to develop the capabilities to comply with the Rules, a **staggered or phased implementation period** may be beneficial as opposed to a single implementation date, as proposed under Rule 1(2). In particular, Rule 10 (which addresses verifiable consent) and Rule 13 (which addresses consent managers) introduce a number of operational expectations that may require complex operational implementation efforts. Accordingly, CIPL asks MeitY to allow Data Fiduciaries sufficient time to operationalize the implementation of such technical requirements.
RULE 2	
Rule 2. Definitions. Unless the context otherwise requires, all expressions shall have the meaning assigned to them in the Digital Personal Data Protection Act, 2023 (22 of 2023) (hereinafter referred to as "Act").	India's Digital Personal Data Protection Act 2023 ("DPDPA" or "the Act") authorizes the government to make rules not inconsistent with the provisions of the Act.[2] Accordingly, CIPL believes that the Act authorizes MeitY to clarify the following provisions: • DPDPA Section 8(3) requires data fiduciaries to ensure completeness and accuracy where personal data is **likely to be disclosed to another data fiduciary** or **likely to be used to make a decision that affects the data principal**. The Act, however, does not define "a decision that affects the data

[2] DPDPA Section 40(1): "The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act."

MeitY DRAFT TEXT	COMMENTS
	principal." CIPL requests MeitY to clarify that a decision affecting a data principal is one that has a legal or similarly significant impact. • DPDPA Section 2(z) defines "**Significant Data Fiduciary**" as any data fiduciary or class of data fiduciaries "as may be notified by the Central Government under section 10." CIPL requests MeitY to provide guidance and/or examples to ensure a better and more uniform understanding of the classification, especially given the additional obligations placed on Significant Data Fiduciaries. Please refer to our additional comments related to Significant Data Fiduciaries under Rule 12. • Relatedly, DPDPA Section 10(1)(a) includes among the factors to be assessed for determining whether an entity is a Significant Data Fiduciary "the **volume and sensitivity** of personal data processed," without an explanation of what qualifies as sensitive personal data. CIPL requests MeitY to provide further clarification, potentially through practical examples. • DPDPA Section 6(1) provides that "consent given by the Data Principal shall be free, specific, informed, **unconditional** and unambiguous …" [emphasis added], but it does not define what types of conditions would render consent invalid. This creates uncertainty for Data Fiduciaries, particularly in cases where digital services—especially free services—depend on ancillary services like advertising. In such scenarios, the main free service often cannot be provided without supplementary services. We argue that the inclusion of such ancillary services as a pre-requisite to processing data / providing the main service should not be viewed as conditions that invalidate consent. If the Consent Notice clearly outlines the purpose of data processing and the Data Principal makes an informed decision and voluntarily agrees to it under the standards of the Indian Contract Act, 1872, this should be treated as "unconditional" consent.

MeitY DRAFT TEXT	COMMENTS
RULE 3	
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, which shall include, at the minimum,— (i) an itemised description of such personal data; and (ii) the specified purpose of, and an itemised description of the goods or services to be provided or uses to be enabled by, such processing; and (c) 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— (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given; (ii) exercise her rights under the Act; and (iii) make a complaint to the Board.	While DPDPA Section 40(2) authorizes the government to make rules about "the **manner** in which the notice [is] given," CIPL is grateful that MeitY has interpreted the ***manner*** of giving notice as including the ***content*** thereof, specifically requiring a description of the personal data to be processed while specifying the purpose for such processing. These elements help to align India's law with the **Global Cross Border Privacy Rules (CBPR) System**, which is a multilateral data transfer mechanism that facilitates trusted personal information flows from and between participating jurisdictions and organizations. We understand that the Indian government has previously expressed an interest in learning more about the Global CBPR System. That said, certain elements of Rule 3, as drafted, appear to be overly prescriptive. By requiring "**at the minimum** … an **itemised** description of the goods or services to be provided or uses to be enabled by, such processing…," the Rule could be interpreted to require unwieldy and long notices that do not benefit Data Principals. Indeed, an unwieldy, itemized description could conflict with the Rule's "clear and plain language" requirement. CIPL requests MeitY to clarify that the required elements of the notice may be incorporated by reference via hyperlinks to more detailed documents. Further, by requiring notice to be given "independently of any other information that has been, is or may be made available by such Data Fiduciary," Rule 3 risks overwhelming users with too much information to the point where users are more likely to accept notices blindly without fully understanding their consequences. Moreover, the Rule's use of the word "purpose" in the singular could be read to require a separate notice for each purpose, thereby contributing to consent and notice fatigue.

MeitY DRAFT TEXT	COMMENTS
	CIPL thus proposes Rule 3 to be redrafted as follows: **[Proposed Revision to] Rule 3. Notice given by Data Fiduciary to Data Principal.** The notice given by the Data Fiduciary to the Data Principal shall be presented in clear and plain language that— (a) provides 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, (b) includes a description of the personal data to be processed; (c) specifies the purpose(s) for such processing; and (d) describes the means by which the Data Principal may— (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given; (ii) exercise her rights under the Act; and (iii) make a complaint to the Board. The above information may be provided by reference to other documents, such as through hyperlinks. CIPL further proposes that MeitY provide examples of how notices should be phrased to assist Data Fiduciaries who may be undertaking this exercise for the first time, and to help global Data Fiduciaries better assess any potential gaps in their existing notices. In addition, MeitY should consider including a new section providing clarity on the employment exemption from consent.[3] The statutory exemption could be read

[3] DPDPA Section 7 sets forth "certain legitimate uses" for which consent is not necessary, including, under subsection (i), "for the purposes of employment …."

MeitY DRAFT TEXT	COMMENTS
	narrowly to apply only to an employer's current workforce, but an employer should not be required to obtain consent from an applicant to collect information necessary to qualify for a job or to conduct background screenings. As such, the Rules should clarify that employment purposes include recruiting and activities related to identifying, referring, assessing, and communicating with and selecting job applications or potential job applicants. Similarly, the Rules should explicitly include payroll, expense monitoring and reimbursement, as well as general employment information needed for enterprise resource planning. We also recommend noting that these same protections apply to independent contractors in the workplace setting. CIPL believes that such clarifications are consistent with the purpose of the employment exemption in Section 7(i) of the Act. Moreover, as drafted, Rule 3 does not clearly specify whether the notice requirements apply to legacy notices. There is no indication of a look-back period for issuing such notices, leading to uncertainty about how Data Fiduciaries should approach legacy data under the current framework. Accordingly, we propose the following measures: • Allow Data Fiduciaries to tie the look-back period for legacy notices to their existing internal data retention policies. For instance, if a company's internal retention policy mandates that Personal Data will be retained for three years, the look-back period for issuing legacy notices should match this three-year timeframe from the date the DPDPA is enforced. • Permit Data Fiduciaries to conduct the look-back process and issue legacy notices on a best-efforts basis. This would offer flexibility, particularly for entities managing vast amounts of historical data, without compromising the overall intent of user transparency. • Amend Rule 3(b) to provide clearer guidance on the specific information that must be included in legacy notices. Additionally, explicit directions on acceptable methods of delivering these notices—such as allowing public notices in certain situations—would help standardize compliance efforts across different sectors.

MeitY DRAFT TEXT	COMMENTS
RULE 4	
Rule 4. Registration and obligations of Consent Manager. (1) A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website. (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. (3) The Consent Manager shall have obligations as specified in Part B of First Schedule. (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.	Pursuant to the DPDPA, a Consent Manager is a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an "**accessible, transparent and interoperable platform**."[4] Every Consent Manager must be registered with the Board and is subject to technical, operational, financial, and other conditions as prescribed.[5] A Consent Manager is accountable to the Data Principal and acts on the Data Principal's behalf, subject to prescribed obligations.[6] The DPDPA also authorizes the government to make rules providing "the manner of accountability and the obligations of Consent Manager."[7] While Rule 4 addresses the registration process and obligations of Consent Managers, CIPL raises concerns regarding the **interoperability** of platforms maintained by different Consent Managers and to what extent such platforms must be interoperable with systems used by Data Fiduciaries. Neither the Rule nor the First Schedule[8] addresses these matters. Clarification on what interoperability looks like could eliminate confusion and forestall potential operational and compliance burdens for Data Fiduciaries and Consent Managers alike. Relatedly, Part B of the First Schedule should clarify whether a Data Fiduciary (acting as the transferor) must provide access to and/or transmit personal data

4 DPDPA Section 2(g).

5 DPDPA Section 6(9): "Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed."

6 DPDPA Section 6(8): "The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed."

7 DPDPA Section 40(2)(c).

8 Part A of the First Schedule addresses the conditions of registration for Consent Managers; Part B addresses the obligations of Consent Managers.

MeitY DRAFT TEXT	COMMENTS
(5) The Board may, if it is satisfied that it is necessary so to do in the interests of Data Principals, after giving the Consent Manager an opportunity of being heard, by order, for reasons to be recorded in writing,— (a) suspend or cancel the registration of such Consent Manager; and (b) give such directions as it may deem fit to that Consent Manager, to protect the interests of the Data Principals. (6) The Board may, for the purposes of this rule, require the Consent Manager to furnish such information as the Board may call for. **FIRST SCHEDULE** **[See rule 4]** **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	through a Consent Manager to another Data Fiduciary (acting as the transferee) solely upon the request of the transferee. Part B should also clarify that any access and/or transfer requests may not authorize the disclosure or transfer of data that would adversely affect the rights—such as privacy, trade secrets, or intellectual property rights—of the Data Fiduciary (as transferor) or third parties. Such an exemption should also cover data created by a Data Fiduciary (as transferor) based on data provided by the Data Principal. For example, user profiles created by a Data Fiduciary should be excluded from the scope of any access/transfer request. Further, to the extent a request may run counter to the principle of data minimization (e.g., potentially requiring a Data Fiduciary to access personal data when it would not necessarily do so otherwise), an exemption should apply. Finally, CIPL asks MietY to clarify that the obligations of a Consent Manager are triggered only when a Consent Management Platform service is used (i.e., a third party service) and not when a company chooses to use its own internal "home grown" solution.

MeitY DRAFT TEXT	COMMENTS
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. **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. Illustration. 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	

MeitY DRAFT TEXT	COMMENTS
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:— (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.	

MeitY DRAFT TEXT	COMMENTS
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, 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	

MeitY DRAFT TEXT	COMMENTS
(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 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).	
RULE 6	
Rule 6. Reasonable security safeguards. (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	Rule 6 requires a Data Fiduciary to take "reasonable security safeguards to prevent personal data breach." The Act defines "personal data breach" as any unauthorised processing of personal data or accidental disclosure, acquisition,

MeitY DRAFT TEXT	COMMENTS
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; (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 data- backups; (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).	sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data."[9] CIPL urges MeitY to replace "at a minimum" with "as appropriate" in the opening clause of Rule 6(1). Use of the word "appropriate" provides organizations with a degree of flexibility to employ context-specific safeguards, CIPL suggests including a reference to established standards or frameworks to help organizations level-set their obligations in India. Rule 6(e)'s requirement to retain access logs and related personal data for one year should be replaced with a similar risk-based approach, giving businesses the flexibility to establish a retention period as appropriate based on risk and the context of use. As drafted, Rule 6(g) introduces unnecessary complexity by appearing to distinguish between "appropriate technical and organizational measures" and "effective observance of security safeguards." CIPL finds this distinction to be unhelpful and unnecessary; we suggest adding a period after "appropriate technical and organizational measures" and striking the remainder of the sentence. CIPL also suggests including a reference to established international standards or frameworks that provide an appropriate standard for the purposes of these Rules.

[9] DPDPA Section 2(u).

MeitY DRAFT TEXT	COMMENTS
RULE 7	
Rule 7. Intimation of personal data breach. (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 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;	Rule 7 requires Data Fiduciaries to convey information about data breaches to affected Data Principals "without delay" upon "becoming aware of any personal data breach." Using "awareness" as the trigger for notifying Data Principals is extremely challenging, given that the notification must include, among other things: • a description of the breach, including its nature, extent and the timing and location of its occurrence; • the consequences likely to arise from the breach relevant to each Data Principal; • the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk; and • the safety measures that Data Principals may take to protect their interests. Conveying such a comprehensive notification merely upon "becoming aware" of a breach is impossible, practically speaking. Appropriate investigation into the cause and extent of the incident, followed by an assessment and implementation of appropriate mitigation measures, must naturally precede any notification that is required to be "concise, clear and plain." Notice issued upon "awareness" will, at best, lack enough relevant information to be useful, or, at worst, contain inaccurate information, potentially exacerbating the situation. In addition, it misdirects resources from engaging in necessary mitigation measures to administrative reporting obligations at a critical time. CIPL urges MeitY to replace the "becoming aware" standard with an alternative standard that contains clear criteria for determining that a breach has, in fact, occurred, and that the breach is "material." Only after determining that a breach has material impact would timely notification be warranted and valuable. A materiality threshold should apply not only to notices for Data Principals under subsection (1), but also to notices to the Board under subsection (2). Requiring

MeitY DRAFT TEXT	COMMENTS
(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.	notification for breaches that have minimal or no impact will result in unnecessary notifications, overwhelming the Board and Data Principals alike. A data breach provision that requires notification to both the Board and data principals in all instances where there has been a breach of personal data is an extremely low threshold. When considered throughout the country as a whole, this has the potential to be unduly burdensome upon businesses, potentially overwhelming to the Board, and causing alarm to data principals, perhaps leading to so-called "notification fatigue." For example, when mandatory breach notification requirements were introduced in the UK, the ICO received about five hundred calls a week and indicated that over-reporting was a problem. We would recommend an approach where notification to the Board and data principals would be required only where unauthorised processing or access has occurred that is likely to result in significant harm to the data principals. This approach would ensure that the Board is fully involved in data incident management, but remains able to respond in serious circumstances without being burdened by numerous trivial but compulsory notifications. It should be noted that the Indian Computer Emergency Response Team (known as "CERT-In") also requires the reporting of security incidents.[10] These are supplemented by sector specific notification requirements, for example, in the payments sector. MeitY should ensure that the breach notification requirements in Rule 7 do not introduce duplications or increased administrative burdens for Data Fiduciaries. Furthermore, the 72-hour notification timeline for reporting breaches to the Board under Rule 7(2) does not take into account the time required for companies—particularly those with global operations—to fully investigate a given incident. In most incidents, time is required to determine what happened, who was affected, and, for global companies, in which country those affected

[10] See https://www.cert-in.org.in/faq.jsp.

MeitY DRAFT TEXT	COMMENTS
	individuals reside. Data Fiduciaries should be allowed flexibility in the 72-hour timeline to reflect the time needed for proper investigation and reporting. CIPL would recommend allowing breach notifications to be issued in phases when all details are not immediately available, and that the Board be informed of confirmed material breaches based on available information, with further updates provided as appropriate. Lastly, it is important to note that many Data Fiduciaries may lack a direct contact point with the Data Principal and may need to rely on an intermediary party in order to communicate effectively with a Data Principal. For example, in many B2B industries, Data Fiduciaries will receive Personal Data from corporate clients and may lack a communication method with the Data Principal. This situation is more dire when the Data Principal lacks a "user account" (as defined in Rule 7(3)) with the relevant Data Fiduciary. The result could pose a significant practical challenge for such Data Fiduciaries to proactively reach out to Data Principals with whom they do not have a routine contact.
RULE 8	
Rule 8. Time period for specified purpose to be deemed as no longer being served. (1) A Data Fiduciary, who is of such class and is processing personal data for such corresponding purposes as are specified in Third Schedule, shall erase such personal data, unless its retention is necessary for compliance with any law for the time being in force, if, for the corresponding time period specified in the said Schedule, the Data Principal neither approaches such Data Fiduciary for the performance of the specified purpose nor exercises her rights in relation to such processing. (2) At least forty-eight hours before completion of the time period for erasure of personal data under this rule, the Data Fiduciary shall inform the Data	Rule 8 addresses the retention and erasure of personal data by Data Fiduciaries, stipulating that personal data must be deleted after a set time established in the Third Schedule unless the Data Principal interacts with the Data Fiduciary or the Data Principal exercises her rights in relation to the processing of the data. Limiting the retention period to three years for purposes such as account creation or transactions, as proposed in the Third Schedule, would negatively impact businesses, particularly e-commerce platforms that use virtual assistants to help users find products over an extended period of time. Such processing is integral to the service provided and spans the user's entire lifecycle on the platform. While CIPL acknowledges that indefinite retention could conflict with the expectations of Data Principals, establishing hard-and-fast time limits is not the

MeitY DRAFT TEXT	COMMENTS
Principal that such personal data shall be erased upon completion of such period, unless she logs into her user account or otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises her rights in relation to the processing of such personal data. (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 she is able to access the services of such Data Fiduciary. **THIRD SCHEDULE**	best approach. The duration for which personal data should be retained depends on several factors, including the data type, its purpose, the services or products involved, and applicable legal and regulatory requirements. Similarly, a requirement that mandates deletion within a specific time frame fails to account for situations where erasure may be complex and unable to be completed within the designated window, such as where joint bank accounts or shared memberships may require the consent of multiple Data Principals before deletion can occur. CIPL would support the adoption of accountability-based safeguards, **including risk assessments and privacy enhancing measures**, for Data Fiduciaries to determine appropriate retention and deletion practices based on context. Additionally, the 48-hour notice requirement set forth in Rule 8(2) is especially challenging on several fronts. For starters, it fails to take into account the situation (as discussed in our comments to Rule 7) where a Data Fiduciary may not have direct communication with a Data Principal, especially where a Data Principal does not have a "user account." Second, it may complicate data minimization practices by impeding the execution of established retention schedules. Third, it may create logistical challenges where a Data Fiduciary has collected personal data for multiple purposes. To that end, Rule 8 and the Third Schedule should be revised to strike the specific time constraints and instead direct Data Fiduciaries to take reasonable steps either to erase the data or to retain the data with privacy enhancing measures (such as anonymization) when the specified purpose for which the data was processed is no longer being served.[11]

S. no.	Class of Data Fiduciaries	Purposes	Time Period
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 her 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	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

[11] DPDPA Section 8(7) [emphasis added] provides:

"A Data Fiduciary shall, unless retention is **necessary** for compliance with any law for the time being in force,—

"(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is **reasonable** to assume that the specified purpose is no longer being served, whichever is earlier; and

"(b) cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for processing to such Data Processor."

MeitY DRAFT TEXT				COMMENTS
		may be used to get money, goods or services		
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 her 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*	
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 her 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*	

MeitY DRAFT TEXT	COMMENTS
RULE 9	
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.	The DPDPA defines a "person" as, inter alia, an individual, a company, or a group of individuals ("an association of persons or a body of individuals, whether incorporated or not").[12] However, it is unclear whether Rule 9's requirement to provide the "business contact information" of a "person" must include the name of a specific individual (such as the Data Protection Officer, if applicable), or whether a webform, generic email address and/or phone number would qualify as "business contact information." CIPL requests that "business contact information" not be interpreted to refer to an individual. Global companies usually have teams assisting with privacy queries from Data Principals and often employ online request forms where Data Principals can make their requests. The business contact requirement should be flexible to reflect this reality. Moreover, global companies must consider how they interact with Data Principals when determining which method to implement for handling privacy requests. If the company operates online or maintains an internet website, one of the methods for submitting those requests will be through its website, such as through a webform, which may be more efficient than a generic email address. Again, the business contact requirement should be flexible to allow for different operations and protocols.

[12] DPDPA Section 2(s).

MeitY DRAFT TEXT	COMMENTS
RULE 10	
Rule 10. Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian (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— (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. Illustration. C is a child, P is her parent, and DF is a Data Fiduciary. A user account of C is sought to be created on the online platform of DF, by processing the personal data of C. Case 1: C informs DF that she is a child. DF shall enable C's parent to identify herself through its website, app or other appropriate means. P identifies herself as the parent and informs DF that she is a registered user on DF's platform and has previously made available her identity and age	The DPDPA requires Data Fiduciaries to obtain the "verifiable consent of the parent … or lawful guardian" before processing any personal data of a child or a person with a disability.[13] While Rule 10 specifies that Data Fiduciaries "shall adopt appropriate technical and organisational measures to ensure that verifiable consent is obtained," the bulk of the Rule addresses measures to ensure that the person providing consent has the authority to do so. Specifically, it requires Data Fiduciaries to exercise "due diligence" when "checking" whether one has authority to provide consent. Rule 10(1) specifies that a Data Fiduciary may refer to either of the following: *(a)* **reliable details of identity and age <u>that the Data Fiduciary already has available</u>** (where, for example, the individual is already a registered user of the Data Fiduciary's service); or *(b)* **voluntarily provided details of identity and age *<u>or a virtual token mapped to the same</u>*** … As drafted, option (b) appears to offer two distinct options: (1) details voluntarily provided by the individual, or (2) a virtual token. CIPL requests MeitY to confirm whether this is a correct reading of Rule 10(1)(b). With regard to persons with disabilities, Data Fiduciaries should be permitted to meet their compliance obligations based on self-declarations and supporting documents provided by individuals claiming guardianship, without conducting independent verification. CIPL seeks further clarification regarding the use of the terms ***identity*** and ***age***. As drafted, Rule 10(1) is unclear whether ***identity*** is meant to refer to identity as

[13] DPDPA Section 9(1): "The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed."

MeitY DRAFT TEXT	COMMENTS
details to DF. Before processing C's personal data for the creation of her user account, DF shall check to confirm that it holds reliable identity and age details of P. Case 2: C informs DF that she is a child. DF shall enable C's parent to identify herself through its website, app or other appropriate means. P identifies herself as the parent and informs DF that she herself is not a registered user on DF's platform. Before processing C's personal data for the creation of her user account, DF shall, by reference to identity and age details issued by an entity entrusted by law or the Government with maintenance of the said details or to a virtual token mapped to the same, check that P is an identifiable adult. P may voluntarily make such details available using the services of a Digital Locker service provider. Case 3: P identifies herself as C's parent and informs DF that she is a registered user on DF's platform and has previously made available her identity and age details to DF. Before processing C's personal data for the creation of her user account, DF shall check to confirm that it holds reliable identity and age details of P. Case 4: P identifies herself as C's parent and informs DF that she herself is not a registered user on DF's platform. Before processing C's personal data for the creation of her user account, DF shall, by reference to identity and age details issued by an entity entrusted by law or the Government with maintenance of the said details or to a virtual token mapped to the same, check that P is an identifiable adult. P may voluntarily make such details available using the services of 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—	parent or guardian. And ***age*** could be interpreted as requiring only confirmation that an individual is an adult (i.e., over the age of 18). Furthermore, while Rule 10 provides several useful illustrations as guidance for Data Fiduciaries, none of the illustrations proposes a situation where an individual falsely claims to be a child or falsely claims to be the parent or guardian. Providing such an example would help clarify how Data Fiduciaries should handle potential misrepresentations and what safeguards should be in place to detect and prevent such cases. Given these uncertainties, CIPL suggests a phased implementation of Rule 10 until there is greater clarity on the age-gating mechanism and the role of the notified Digital Locker service provider. Indeed, these provisions should not go into effect until the government has established a workable Digital Locker service provider program. Additionally, CIPL requests further explanation of the existing Digital Locker infrastructure, particularly how it supports the verification of guardianship and its interaction with age token verification. The potential application of the Digital Locker mechanism for age verification may involve complex implementation efforts that require further guidance on practical execution. CIPL also notes that there is a helpful exemption for obtaining consent for children for education. Many companies also provide education and skills building services either through schools or other programs aimed at areas like digital literacy. These services can involve children, but are low-risk educational services similar to those provided by schools. CIPL suggests expanding the exemption to also include educational and skills building services provided by Data Fiduciaries. While the DPDPA does not make a distinction regarding the age of a child for obtaining verifiable parental consent, the Rules should consider requiring verifiable parental consent for teens (ages 13-17) only for high-risk situations, such as when the Data Fiduciary's product or service is primarily designed to enable (i) social interaction; (ii) the creation and sharing of user-created content; and (iii) engagement with content via algorithmic recommendations.

MeitY DRAFT TEXT	COMMENTS
(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 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	To further ease compliance efforts, we propose that the Government explicitly clarify that the requirement to obtain verifiable parental consent applies only to new instances of data processing involving children. This means that: • Legacy data collected before the implementation of the DPDPA and the Rules should not require (retrospective) parental consent. • Re-consent / fresh content should not be mandatory when a child reaches adulthood, unless consent earlier given was withdrawn before adulthood.

MeitY DRAFT TEXT	COMMENTS
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	
Rule 11. Exemptions from certain obligations applicable to processing of personal data of child. (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.	While we commend the Government for allowing specific exemptions under Rule 11 read with Schedule IV, we respectfully recommend broadening the scope of exempted purposes to explicitly include "personalization of services" that do not otherwise have detrimental effects on children. Personalization plays a key role in enhancing user engagement and ensuring that content and services align with the needs and preferences of individual users. For children, this could mean receiving age-appropriate educational materials, entertainment options, or safety prompts that enhance their online experience. It is important to note that such personalization would still be subject to the overarching safeguard outlined in Section 9(2) of the DPDPA, which prohibits any form of data processing that could have a detrimental impact on the well-being of a child. Furthermore, we recommend the Rules clarify that the prohibition on targeted ads under Section 9(3) does not extend to ads that do not involve processing a child's Personal Data, apart from details like age and location. MietY should also consider amending Part B of the Fourth Schedule to provide additional exceptions for products and services that are low risk.

MeitY DRAFT TEXT	COMMENTS
RULE 12	
Rule 12. Additional obligations of Significant Data Fiduciary. (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 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.	Rule 12(3) requires a Significant Data Fiduciary to verify that any algorithmic software deployed by it is "not likely to pose a risk to the rights of Data Principals." As drafted, this provision could be interpreted to mean that ***any*** risk associated with the use of algorithmic software is unacceptable. Such a strict interpretation could create substantial challenges for the implementation and use of AI and other technologies relying on algorithms, and it may conflict with other legal obligations that require the use of algorithmic tools, such as for content moderation. Therefore, MeitY should consider modifying Rule 12(3) to either delete the reference to algorithmic software (as it will likely be addressed in a separate emerging regulatory framework), or limit it to address situations that pose **significant risk**. More generally, Rule 12 imposes heightened obligations on companies that require significant investment. MeitY should therefore provide guidance establishing a clear threshold for an entity's designation as a "Significant Data Fiduciary" (SDF) so that companies may anticipate and appropriately prepare for these heightened obligations. MeitY also should clarify that service providers are not SDFs merely because of the processing activities they undertake on behalf of a Data Fiduciary. Given that Rules 12(1) and 12(2) require the SDF to conduct both a Data Protection Impact Assessment (DPIA) and an audit, MeitY should clarify the differences between DPIAs and audits (since audits routinely supply DPIAs as supporting documents) and clarify the circumstances for which a DPIA or audit would be required. For example, should they be conducted for specific processing activities or for processing as a whole? Should they be conducted periodically or only when significant changes occur?

MeitY DRAFT TEXT	COMMENTS
	Furthermore, MeitY should provide additional guidance regarding the required audit. CIPL would suggest that self-audit be an option, provided that specified standards for the structure of the assessment are met and the SDF is willing to certify and/or attest to its findings. As for DPIAs, we understand that the intention of the Rules is not to have DPIAs conducted externally, but we ask for the Rules to make that explicit. It would be challenging and atypical for a DPIA to be conducted by an external party. The SDF is best placed to conduct DPIAs internally on an on-going basis, as part of its privacy by design process. It would be appropriate for an SDF, and not a third party, to adequately assess the scope of the processing activity as well as the potential impact of the processing activity to the rights of data principals. Rule 12(1)'s requirement for DPIAs and audits to be conducted on an annual basis may not achieve any effective or meaningful results. This may be treated by most entities as another "check-the-box" compliance obligation instead of approaching it from the perspective of whether the activities result in any incremental harm to data principals. To illustrate, should a multinational company be classified as an SDF where it processes only employee data, under the Rules as drafted, the company would be required to conduct a DPIA every 12 months even though its personal data processing activities (e.g. maintenance of HR records, compensation and payroll requirements) remain the same. Mandating an annual DPIA would also result in processors being subject to annual reviews by SDFs even when their role and scope of processing remains unchanged. This would result in added compliance obligations, resulting in added costs which would be passed on to consumers. Conceptually, a DPIA is a key component of a Privacy by Design approach, in which organizations consider the protection of personal data from the earliest possible design stage, and throughout the operational life cycle, of the new

MeitY DRAFT TEXT	COMMENTS
	system, process, product, or service. As such, we recommend taking a more pragmatic and effective approach to the conduct of a DPIA. We suggest mandating a DPIA only: (a) for processing activities likely to result in a high risk of harm to data principals; and (b) whenever there is any material change in the methodology, technology, or process relating to the processing activity that may potentially result in an increased risk of harm to the data principals. Further, we recommend that multiple processing activities that are similar in purpose, scope, and context can be covered in a single DPIA. As for Rule 12(4), which requires SDFs to comply with data localization restrictions, CIPL strongly opposes the introduction of data localization requirements. [See our commentary in response to Rule 14.] However, to the extent such restrictions remain, MeitY should provide examples of data localization measures and better explain localized traffic flows to ensure a clear understanding of compliance requirements. Moreover, MeitY should be aware of the potential impact of data localization restrictions on certain sectors, such as the pharmaceutical industry, which must report clinical trial results to various governments worldwide, regardless of where the data is collected. Finally, MeitY should clarify whether these localization rules will prevent certain profiles of data from leaving the country, or whether such rules will allow transfers as long as a local copy is retained. Unnecessarily restricting the free flow of data is likely to have a negative impact on the economy and many commercially and socially beneficial services, which rely on the ability to move data. Rather than focusing on data localization, MeitY should align with other global data transfer mechanisms and frameworks such as the Global Cross-Border Privacy Rules (Global CBPR) and Global Privacy Recognition for Processors (Global PRP) to protect data while facilitating free data flows that are integral to India's digital economy. We urge that the "committee" referenced in Rule 12(4) focus its efforts on enabling free flows of data with trust.

MeitY DRAFT TEXT	COMMENTS
RULE 13	
Rule 13. Rights of Data Principals. (1) For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager, shall publish on its website or app, or both, as the case may be, — (a) the details of the means using which a Data Principal may make a request for the exercise of such rights; and (b) the particulars, if any, such as the username or other identifier of such a Data Principal, which may be required to identify her under its terms of service. (2) To exercise the rights of the Data Principal under the Act to access information about personal data and its erasure, she may make a request to the Data Fiduciary to whom she has previously given consent for processing of her personal data, using the means and furnishing the particulars published by such Data Fiduciary for the exercise of such rights. (3) Every Data Fiduciary and Consent Manager shall publish on its website or app, or both, as the case may be, the period under its grievance redressal system for responding to the grievances of Data Principals and shall, for ensuring the effectiveness of the system in responding within such period, implement appropriate technical and organisational measures. (4) To exercise the rights of the Data Principal under the Act to nominate, she may, in accordance with the terms of service of the Data Fiduciary and such law as may be applicable, nominate one or more individuals, using the means and furnishing the particulars published by such Data Fiduciary for the exercise of such right. (5) In this rule, the expression "identifier" shall mean any sequence of characters issued by the Data Fiduciary to identify the Data Principal and includes a customer identification file number, customer acquisition form number,	MeitY should clarify the means by which a Data Principal may nominate one or more individuals to exercise the Data Principal's rights, as well as how Data Fiduciaries should recognize the appointment of such surrogates in practice. Further guidance is also needed on the role of Consent Managers in facilitating a Data Principal's rights, particularly in relation to Rule 10 (Verifiable consent of a guardian before processing the personal data of children). Consent Managers are a key component of the techno-legal regulatory framework under the DPDPA, and additional guidance would be beneficial regarding their operationalization. In particular, CIPL seeks clarification as to whether Data Fiduciaries are required to ensure interoperability with all Consent Managers through APIs or similar technical solutions. As noted earlier in our comments to Rule 4, clarification on what interoperability looks like could eliminate confusion and forestall potential operational and compliance burdens for Data Fiduciaries and Consent Managers alike. Additionally, clarification is needed on whether Data Fiduciaries can continue using their existing consent interfaces for interactions with Data Principals, including those provided by group companies, alongside mechanisms facilitated by Consent Managers. Clarification on these aspects would help ensure that the nomination process under Rule 13(4) is effectively implemented while maintaining consistency across different Data Fiduciaries and Consent Managers. Lastly, we respectfully submit that the Rules should strive to establish a fair balance between the rights of Data Principals and the legal and commercial interests of Data Fiduciaries. Without this balance, Data Fiduciaries and their processors may be left vulnerable to risks that could impact their operations, security, and proprietary information. By including specific grounds under which a Data Fiduciary can reject a Data Principal's request— e.g., where requests infringe upon the legal rights of the

MeitY DRAFT TEXT	COMMENTS
application reference number, enrolment ID or licence number that enables such identification.	Data Fiduciary or its data processors, compromise data security or system integrity, lead to the exposure of trade secrets or sensitive commercial information, or are deemed excessive or unreasonable—the law would not only be able to maintain and protect Data Principals' rights but also ensure that Data Fiduciaries are not placed in legally or commercially disadvantageous positions.
RULE 14	
Rule 14. Processing of personal data outside India. 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.	Rule 14 introduces restrictions on the transfer of personal data outside India, especially where personal data would be made available to foreign states or entities under their control. This rule applies to Data Fiduciaries processing data either within India or outside India when related to offering goods or services to Data Principals within India. Specifically, Rule 14 establishes that the transfer of personal data outside India—whether processed within India or outside but in connection with offering goods or services to individuals in India—is subject to specific requirements that may be issued by the Indian Government through general or special orders. However, this broad definition of data transfer raises concerns regarding its potential extraterritorial scope, which could create uncertainty for international organizations. For example, the rule's reference to "any person or entity under the control of or any agency of such State" lacks clarity, particularly in scenarios where data sharing occurs due to legal requirements in foreign jurisdictions. CIPL believes further clarification is needed on whether the sharing of Indian customer data, obtained from an India-based subsidiary, with a parent company for compliance with U.S. financial regulations (e.g., those set by the U.S. Office of Foreign Assets Control, OFAC), would be subject to the restrictions outlined in this Rule.

MeitY DRAFT TEXT	COMMENTS
	Additionally, Rule 12(4), which is related to Rule 14, grants the Indian government authority to mandate localization of certain types of personal data for Significant Data Fiduciaries. From the various public consultation sessions held by MeitY in this regard, we understand that the intention of including these provisions was to specify a process by which the Central Government could give effect to Section 16. However, as drafted, the Rules could be interpreted to extend beyond Section 16 and be seen as reintroducing a strict data localization requirement. While ensuring the protection of personal data is a legitimate objective, imposing additional data localization measures could create operational challenges, particularly for multinational companies that have already implemented robust global data protection frameworks. Reintroduction of data localization requirements, coupled with the uncertainty of the potential types of personal data that may be restricted from transfers, could result in a number of unintended practical, operational and legal challenges and consequences.[14] Instead of introducing localization requirements, we recommend that MeitY adopt binding cross-border data transfer mechanisms such as standard and model contractual clauses, binding corporate rules, codes of conduct, and certifications. These mechanisms are already widely recognized, and CIPL believes that they would facilitate the secure and efficient transfer of data across borders while maintaining strong privacy protections for Data Principals. As noted in our comments to Rule 3, we understand that the Indian government has previously expressed an interest in learning more about the **Global Cross-Border Privacy Rules (Global CBPR) System**, a multilateral data transfer mechanism that facilitates trusted personal information flows from and between participating jurisdictions and organizations. The Global CBPR System is based on

[14] See CIPL-TLS Discussion Paper I: The Real Life Harms of Data Localization Policies, March 29, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf.

MeitY DRAFT TEXT	COMMENTS
	formal third-party assessments affirming that certified organizations adhere to a common set of approved standards. The **Global Privacy Recognition for Processors (Global PRP) System** provides analogous certifications for private sector organizations operating as data processors. CIPL believes that Rule 14 adds a layer of complexity to India's potential participation in the Global CBPR, for it imposes governmental restrictions on personal data leaving India. Although the Global CBPR System does not specifically address access issues by foreign governments, the Global CBPR Forum[15] plans to address the issue in due course. Furthermore, compliance with Rule 14 may pose significant challenges for smaller entities, which may lack the resources to navigate complex regulatory requirements. Clear guidelines and support measures should be provided to ensure SMEs can effectively comply with these obligations without undue burden. It is also worth noting that there are existing sectoral regulations imposing specific data localization requirements, for instance the Reserve Bank of India (RBI) rules on localization of payments data within India.[16] Therefore, additional data localization requirements stemming from Rule 14 would add a layer of complexity and adversely impact the operations of India's financial sector. In addition, it is unclear what would happen if the Indian government were to mandate the localization of certain categories of personal data, such as clinical trial data, within India. Pharmaceutical companies would then need to ensure that their practices comply with Rule 14, meeting any requirements specified by the Central Government for making such data available to foreign entities. This could lead to complexity and administrative burdens, as companies would need to report clinical trial results to various governments worldwide, regardless of where

[15] The Global CBPR Forum is a group of jurisdictions with administrative, operational, and oversight functions with respect to the Global CBPR and Global PRP Systems. See https://www.globalcbpr.org/.

[16] See, for example, Storage of Payment System Data, available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244.

MeitY DRAFT TEXT	COMMENTS
	the data is collected—both for regulatory approval of medicinal products and for adverse event reporting. Therefore, CIPL seeks further clarification and guidance regarding the specific categories or types of personal data that are required to be localized within India. We suggest that a **balanced approach** be taken, which would also address some unintended consequences of data localization. To that end, we propose the following: (a) Rule 12(4) should be modified to reflect that an SDF would only be restricted from transferring specified data to the countries notified under Section 16. (b) Rule 14 should be amended to explicitly recognize lawful data transfer mechanisms that align with global standards—such as standard data protection clauses, binding corporate rules, certification mechanisms, or binding schemes such as Global CBPR and Global PRP—thereby ensuring that personal data remains protected while enabling India to remain an active participant in the global digital economy. (c) Provide further clarification regarding the scope of entities considered to be "under the control" of a foreign state to prevent unintended restrictions on legitimate data-sharing activities required by international regulatory obligations. (d) Provide that any data specified by the Central Government under Rule 12(4), and any restrictions under Rule 14, be subject to such designation following a consultation with affected data fiduciaries and the relevant sectoral regulators. For example, potential restrictions on data transfers could be limited to personal data used for national security purposes. This would allow for a more targeted requirement with a legitimate use case, and should not include personal data or use cases which have everyday commercial applications such as cross-border commerce and transactions. Allowing consultation would also allow valid and legitimate use cases to be discussed in order to help the Central Government identify valid exceptions. Such dialogue will also help to develop mutual understanding

MeitY DRAFT TEXT	COMMENTS
	amongst the parties. Only upon completion of such consultation, should appropriate categories of personal data or purposes of personal data processing be designated by the Central Government, which would include “traffic data” as mentioned in Rule 12(4) to the extent such data is personal data, and relevant sectoral regulators. This would avoid the unintended negative consequences which we have outlined above.