**Interplay of DPDP Act with Competition Act and Draft DCB**

- Territorial application: The processing of personal data must be within the Indian territory or if outside, should be in connection with any activity related to the offering goods and services to individuals within the Indian territory.
- One significant change introduced in the DPDP Act is that it does not categorize data under different heads e.g., sensitive personal data (as identified under the SPDI Rules) or critical personal data (as was proposed in an earlier iteration of the draft data protection bill) depending on sensitivity of the personal data.
- The DPDP Act permits cross-border data transfers to all countries, unless restricted by the Central Government by notification, as compared to the 2022 Draft Bill permitting data transfers only to countries falling within a government white list.
- The DPDA is more limited in substantive scope than the EU's General Data Protection Regulation (GDPR). While the GDPR applies to all forms of personal data, the DPA applies only to personal data in digital form or non-personal data that is digitized subsequently - though whether this makes any practical difference, given the digitisation of almost all data, is doubtful.
- Any subsidiary in India, like any subsidiary in the EU u/GDPR, will be required to comply with the Act when processing the personal information of its own future, current, and former employees (HR Data) as well as when processing HR Data received from other jurisdictions — for example, a manager in India handling HR Data for subordinates in the United States.
- Jurisdictional/subject matter overlap with the Competition Act? When WhatsApp mandated acceptance of its privacy policy for its users to continue using WhatsApp, the CCI stepped in and initiated an investigation. Interestingly, the CCI emphasized how consent for sharing user data needs to be 'free', 'optional', 'well informed', and 'without withdrawal of services', failing which it may be considered as an imposition of unfair conditions by a dominant undertaking under section 4 of the Competition Act.
- Jurisdictional/subject matter overlap with Consumer Protection Act - unfair trade practices. But there, the nature of remedy is somewhat different from that under this Act or the Competition Act and therefore, the overlap can be sustained.
- The DPDP Act fails to address this regulatory dilemma too – whether companies will be reporting data breaches to the Board or to CERT-In (the nodal agency tasked with addressing cyber incidents, under Section 70B of the IT Act and associated rules). Companies are mandated to report cyber incidents to CERT-In within 6 hours.
- The Data Protection Board of India is the adjudicatory body under the DPDP Act. Appeals against the orders of the Board will lie before the Telecom Disputes Settlement and Appellate Tribunal.

- The Board is designed to function as an adjudicatory body and does not have regulatory functions. This differs from previous iterations of the legislation in 2019 and 2021, which tasked the data protection authority with regulatory functions as well.
- The constitution of the Board may run into trouble with the *Madras Bar Assn* line of cases for failing to have any Judicial member.
- The Board shall have the same investigative powers as a civil court. However, it has not been given the authority to prevent access to any premises or take into custody any equipment which might hinder the daily functioning of an entity.

| **Subject** | **DPDP Act** | **Draft DCB** |
|---|---|---|
| **Application** | **3 (a)** apply to the processing of digital personal data within the territory of India where the personal data is collected—<br>(i) in digital form; or<br>(ii) in non-digital form and digitized subsequently;<br><br>**(b)** also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;<br><br>**(c)** not apply to—<br>(i) personal data processed by an individual for any personal or domestic purpose; and<br>(ii) personal data that is made or caused to be made publicly available by—<br>(A) the Data Principal to whom such personal data relates; or | **3 (2)** An enterprise shall be deemed to be a Systemically Significant Digital Enterprise in respect of a Core Digital Service, if:<br><br>(a) it meets any of the following financial thresholds in each of the immediately preceding three financial years:<br>(i) turnover in India of not less than INR 4000 crore; OR<br>(ii) global turnover of not less than USD 30 billion; OR<br>(iii) gross merchandise value in India of not less than INR 16000 crore; OR<br>(iv) global market capitalisation of not less than USD 75 billion, or its equivalent fair value of not less than USD 75 billion calculated in such manner as may be prescribed;<br><br>AND |

| | | |
|---|---|---|
| | (B) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available. | (b) it meets any of the following user thresholds in each of the immediately preceding three financial years in India:<br>(i) the core digital service provided by the enterprise has at least one crore end users; OR<br>(ii) the core digital service provided by the enterprise has at least ten thousand business users.<br>Provided that if the enterprise does not maintain or fails to furnish data mentioned in clause (a) or (b), it shall be deemed to be a Systemically Significant Digital Enterprise if it meets any of the thresholds stipulated in clause (a) or (b).<br><br>**3 (3)** The Commission may designate an enterprise as a Systemically Significant Digital Enterprise in respect of a Core Digital Service, even if it does not meet the criteria set out under sub-section (2), if the Commission is of the opinion that such enterprise has significant presence in respect of such a Core Digital Service, based on an assessment of information available with it, and based on any or all of the following factors:<br><br>(i) volume of commerce of the enterprise;<br>(ii) size and resources of the enterprise; |

| | | |
|---|---|---|
| | | (iii) number of business users or end users of the enterprise;<br>(iv) economic power of the enterprise;<br>(v) integration or inter-linkages of the enterprise with regard to the multiple sides of market;<br>(vi) dependence of end users or business users on the enterprise;<br>(vii) monopoly position whether acquired as a result of any statute or by virtue of being a Government company or a public sector undertaking or otherwise;<br>(viii) barriers to entry or expansion including regulatory barriers, financial risk, high cost of entry, marketing costs, technical entry barriers, barriers related to data leveraging, economies of scale and scope, high cost of substitutable goods or services for end users or business users;<br>(ix) extent of business user or end user lock in, including switching costs and behavioral bias impacting their ability to switch or multi-home;<br>(x) network effects and data driven advantages;<br>(xi) scale and scope of the activities of the enterprise;<br>(xii) countervailing buying power;<br>(xiii) structural business or service characteristics;<br>(xiv) social obligations and social costs;<br>(xv) market structure and size of the market; and<br>(xvi) any other factor which the Commission may consider relevant for the assessment. |

| | | |
|---|---|---|
| **Obligations on the regulated entity** | **4 (1)** A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—<br>(a) for which the Data Principal has given her consent; or<br>(b) for certain legitimate uses.<br><br>**(2)** For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.<br><br>**5 (1)** Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her,—<br>(i) the personal data and the purpose for which the same is proposed to be processed;<br>(ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and<br>(iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed.<br><br>**(2)** Where a Data Principal has given her consent for the processing of her personal data before the date of commencement of this Act -<br>(b) the Data Fiduciary may continue to process the | **9 (1)** A Systemically Significant Digital Enterprise shall establish transparent and effective complaint handling and compliance mechanisms as may be specified.<br><br>**12 (2)** A Systemically Significant Digital Enterprise shall not, without the consent of the end users or business users:<br><br>(a) intermix or cross use the personal data of end users or business users collected from different services including its Core Digital Service; or<br>(b) permit usage of such data by any third party.<br><br>Explanation.— For the purposes of this subsection, "consent":<br><br>(1) For end users, shall have the same meaning as assigned to it in the Digital Personal Data Protection Act, 2023 (22 of 2023);<br>(2) For business users, shall have the same meaning as may be specified. |

| | | |
|---|---|---|
| | personal data until and unless the Data Principal withdraws her consent.<br><br>---<br><br>**6 (1)** The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify 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.<br><br>**(4)** Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.<br><br>**(5)** The consequences of the withdrawal referred to in sub-section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.<br><br>**(6)** If a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease | |

| | | |
|---|---|---|
| | processing the personal data of such Data Principal unless such processing without her consent is required or authorized under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.<br><br>(7) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.<br><br>(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.<br><br>(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.<br><br>---<br><br>**7.** A Data Fiduciary may process personal data for uses, namely:—<br><br>(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal | |

| | | |
|---|---|---|
| | data.<br><br>(b) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, license or permit as may be prescribed…<br><br>(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;<br><br>(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;<br><br>(e) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;<br><br>(f) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other | |

| | | |
|---|---|---|
| | individual;<br><br>(g) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;<br><br>(h) for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order;<br><br>(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.<br><br>---<br><br>**8 (7)** A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—<br>(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<br>(b) cause its Data Processor to erase any personal | |

| | | |
|---|---|---|
| | data that was made available by the Data Fiduciary for processing to such Data Processor.<br><br>**(10)** A Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals.<br><br>---<br><br>**10 (1)** The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including—<br><br>(a) the volume and sensitivity of personal data processed;<br>(b) risk to the rights of Data Principal;<br>(c) potential impact on the sovereignty and integrity of India;<br>(d) risk to electoral democracy;<br>(e) security of the State; and<br>(f) public order<br><br>**(2)** The Significant Data Fiduciary shall—<br><br>(a) appoint a Data Protection Officer who shall—<br>(i) represent the Significant Data Fiduciary under the provisions of this Act;<br>(ii) be based in India; | |

| | | |
|---|---|---|
| | (iii) be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary; and<br>(iv) be the point of contact for the grievance redressal mechanism under the provisions of this Act;<br><br>(b) appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act; and<br><br>(c) undertake the following other measures, namely:—<br><br>(i) periodic Data Protection Impact Assessment, which shall be a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed;<br>(ii) periodic audit; and<br>(iii) such other measures, consistent with the provisions of this Act, as may be prescribed. | |
| **Exemption** | **17 (1)** The provisions of Chapter II, except sub-sections (1) and (5) of section 8, and those of Chapter III and section 16 shall not apply where— | **38.** Power of the Central Government to exempt enterprises - The Central Government may, by notification, exempt an enterprise from the application of one or more provisions of this Act, |

| | | |
|---|---|---|
| | (a) the processing of personal data is necessary for enforcing any legal right or claim;<br>(b) the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function;<br>(c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offense or contravention of any law for the time being in force in India;<br>(d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India;<br>(e) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force; and<br>(f) the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing | the rules or regulations framed thereunder, or any provision thereof, and for such period as it may specify in such notification:<br><br>(a) in the interest of security of the State or public interest;<br>(b) in accordance with any obligation assumed by India under any treaty, agreement or convention with any other country or countries.<br>(c) if it performs a sovereign function on behalf of the Central Government or a State Government, only in respect of activities relatable to the discharge of the sovereign functions. |

| | | |
|---|---|---|
| | being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.<br><br>Explanation.—For the purposes of this clause, the expressions "default" and "financial institution" shall have the meanings respectively assigned to them in sub-sections (12) and (14) of section 3 of the Insolvency and Bankruptcy Code, 2016.<br><br>**(2)** The provisions of this Act shall not apply in respect of the processing of personal data—<br><br>(a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offense relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and<br>(b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.<br><br>**(3)** The Central Government may, having regard to the volume and nature of personal data processed, | |

| | | |
|---|---|---|
| | notify certain Data Fiduciaries or class of Data Fiduciaries, including startups, as Data Fiduciaries to whom the provisions of section 5, sub-sections (3) and (7) of section 8 and sections 10 and 11 shall not apply.<br><br>**(4)** In respect of processing by the State or any instrumentality of the State, the provisions of sub-section (7) of section 8 and sub-section (3) of section 12 and, where such processing is for a purpose that does not include making of a decision that affects the Data Principal, sub-section (2) of section 12 shall not apply.<br><br>**(5)** The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification. | |
| **Board/Authority** | **23 (2)** No act or proceeding of the Board shall be invalid merely by reason of—<br><br>(a) any vacancy in or any defect in the constitution of the Board;<br>(b) any defect in the appointment of a person acting as the Chairperson or other Member of the Board; or<br>(c) any irregularity in the procedure of the Board, | Competition Commission. |

| | | |
|---|---|---|
| | which does not affect the merits of the case.<br><br>---<br><br>**28 (7)** For the purposes of discharging its functions under this Act, the Board shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to—<br><br>(a) summoning and enforcing the attendance of any person and examining her on oath;<br>(b) receiving evidence of affidavit requiring the discovery and production of documents;<br>(c) inspecting any data, book, document, register, books of account or any other document; and<br>(d) such other matters as may be prescribed.<br><br>**(8)** The Board or its officers shall not prevent access to any premises or take into custody any equipment or any item that may adversely affect the day-to-day functioning of a person. | |
| **Penalty** | **33 (1)** If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may…impose such monetary penalty specified in the Schedule.* | **28 (1)** In an order finding a contravention under sub-section (1) of Section 17, the Commission may impose on a Systemically Significant Digital Enterprise or its Associate Digital Enterprise, penalties not exceeding ten per cent of its global turnover, in the preceding financial year where it finds that the Systemically Significant Digital |

| | | |
|---|---|---|
| | | Enterprise or its Associate Digital Enterprise, fails to comply with any of the obligations laid down in Chapter III and the rules and regulations framed thereunder.<br><br>**(2)** In an order finding a contravention under sub-section (3) of Section 5, the Commission may impose on a Systemically Significant Digital Enterprise or its Associate Digital Enterprise, penalties not exceeding ten per cent of its global turnover, in the preceding financial year where it finds that the Systemically Significant Digital Enterprise or its Associate Digital Enterprise, fails to comply with the obligation under sub-section (1) of Section 5.<br><br>**(3)** The Commission may pass an order, imposing on an enterprise a penalty where applicable which shall not exceed one percent of the global turnover of such an enterprise where they fail to notify the Commission that they meet the criteria specified in sub-section (2) of Section 3 and the notifications issued thereunder.<br><br>**(4)** The Commission may pass an order, imposing on an enterprise a penalty, which shall not exceed one per cent of the global turnover of the enterprise, where it:<br>(a) provides incorrect, incomplete or misleading information or no information under sub-section |

| | | |
|---|---|---|
| | | (1) or sub-section (3) of Section 4;<br>(b) fails to provide information, or supplies incorrect, incomplete or<br>misleading information that is required pursuant to a show cause<br>notice under Section 4 or Section 16;<br>(c) provides or supplies incorrect, incomplete or misleading information<br>under sub-section (1) of Section 6;<br>(d) fails to provide information, or provides or supplies incorrect,<br>incomplete or misleading information under sub-section (2) of Section 9;<br>(e) provides incorrect, incomplete or misleading information, or fails to or refuses to provide complete information or cooperate pursuant to the powers of the Commission under Section 21 or the Director General under Section 24. |

*** Schedule :**

THE SCHEDULE

[*See* section 33 (*1*)]

| Sl. No. | Breach of provisions of this Act or rules made thereunder | Penalty |
|---|---|---|
| (1) | (2) | (3) |
| 1. | Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (*5*) of section 8. | May extend to two hundred and fifty crore rupees. |
| 2. | Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (*6*) of section 8. | May extend to two hundred crore rupees. |
| 3. | Breach in observance of additional obligations in relation to children under section 9. | May extend to two hundred crore rupees. |
| 4. | Breach in observance of additional obligations of Significant Data Fiduciary under section 10. | May extend to one hundred and fifty crore rupees. |
| 5. | Breach in observance of the duties under section 15. | May extend to ten thousand rupees. |
| 6. | Breach of any term of voluntary undertaking accepted by the Board under section 32. | Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted. |
| 7. | Breach of any other provision of this Act or the rules made thereunder. | May extend to fifty crore rupees. |