NAVIGATING INDIA'S DATA PROTECTION LANDSCAPE: A BRIEF OVERVIEW AND ACTIONABLE INSIGHTS

*By **Namit Oberoi* & Niharika Mehra*****

** Chief Manager, Legal Team, Times Internet Limited, Noida, India*

*** Contracting Manager, Accenture, Gurugram, India*

In the dynamic realm of digital information, India has embarked on a journey to fortify the safeguards around personal data through its evolving data protection laws. The genesis of this initiative can be traced back to the Supreme Court seminal judgment in the Puttaswamy case which led to the various iterations of the Personal Data Protection Bills, finally culminating in the Personal Data Protection Act, 2023. As we stand on the cusp of a new era in data governance, businesses operating within India must proactively adapt to comply with the stringent provisions set forth by the legislation. This article serves as a comprehensive guide, offering actionable insights and a compliance checklist to empower companies in aligning their practices with the requirements of India's new data protection law.

Detailed Compliance checklist for businesses under the Digital Personal Data Protection Act, 2023

S. No.	Compliance required	Details	To be clarified in Rules
1.	Processing data only for lawful purpose with consent (Clause 4)	**Lawful Purpose**: Data Fiduciary can only process the personal data of a data principal in accordance with the Act and for a lawful purpose i.e., which is not expressly forbidden by law. This lawful purpose can either be with the consent of the data principal or for certain legitimate uses.	

2.	Provide notice for consent. (Clause 5)	**Notice and Consent:** Data Fiduciary must provide a notice to the Data Principal seeking it consent. The notice should include information about the personal data being processed, the purpose of processing, consent withdrawal, grievance redressal mechanism and the process of making complaint to the Board. The aforesaid consent requirement is also required to be followed by the Data Fiduciary if the Data Principal has already given consent before commencement of the Act. The notice should be in English, or any language specified in the Eighth Schedule to the Constitution. **Withdrawal of Consent:** Data Fiduciary is allowed to continue processing the personal data until the Data Principal withdraws their consent.	The manner in which the notice is to be given by the Data Fiduciary to a Data Principal
3.	Regarding Consent (Clause 6)	**Requirements for Consent:** Consent must be free, specific, informed, unconditional, and unambiguous, with a clear affirmative action signifying acceptance for processing of personal data for the specified purpose and must be limited to processing of personal data for such purpose. If any part of the consent infringes any law, then it shall be invalid. **Clear and plain language**: Requests for consent must be presented in clear and plain language in English or any language specified in the Eighth Schedule to the Constitution. Data Fiduciary must provide the Contact details of a Data Protection Officer/authorized person who can respond to communication with the Data Principal.	

		Right to withdraw consent: Data Principals have the right to withdraw their consent at any time, with the ease of withdrawal comparable to the ease of giving consent. The legality of processing based on consent before withdrawal is not affected. **Cease processing upon withdrawal:** If a Data Principal withdraws consent, the Data Fiduciary must cease and also ensure its Data Processors cease processing the personal data within a reasonable time, unless processing without consent is required/authorized under law. **Consent Manager:** Consent can be given, managed, reviewed, or withdrawn through a Consent Manager by the Data Principal. The Consent Manager is accountable to the Data Principal and acts on their behalf, subject to prescribed obligations. Consent Managers must be registered with the Board and comply with prescribed conditions. **Proof of consent:** In case of a question regarding the basis of processing personal data, the Data Fiduciary must prove that a notice was given to the Data Principal and consent was obtained in accordance with the Act and rules.	The manner of accountability and the obligations of Consent Manager. The manner of registration of Consent Manager and the conditions relating thereto
4.	Legitimate uses (Clause 7)	Data Fiduciary can process personal data for legitimate uses as explained below: **Specified Purpose**: The Data Fiduciary can process personal data if it is provided voluntarily by the Data Principal for a specified purpose, and the Data Principal has not indicated that they do not consent to the use of their personal data.	

		Obligations under Law: The Data Fiduciary can process personal data to fulfill any obligation under law and to comply with judgments, decrees, or orders. **Employment and Safeguarding**: The Data Fiduciary can process personal data for employment purposes or to safeguard the employer from loss or liability, such as preventing corporate espionage, maintaining confidentiality of trade secrets, intellectual property, or classified information, or providing services or benefits to employee Data Principals.	
5.	Obligations of data fiduciary (Clause 8)	**Responsibility for Compliance**: A Data Fiduciary is responsible for complying with the provisions of the Act and the rules made under it, regardless of any agreement or failure of the Data Principal to fulfill their duties. **Mandatory contract with Data Processors**: A Data Fiduciary can engage a Data Processor to process personal data on its behalf, but only under a valid contract. **Ensuring Completeness, Accuracy, and Consistency**: If personal data processed by a Data Fiduciary is likely to be used to make a decision that affects the Data Principal or disclosed to another Data Fiduciary, the Data Fiduciary must ensure the completeness, accuracy, and consistency of the data. **Implementing Technical and Organizational Measures**: A Data Fiduciary must implement appropriate technical and organizational measures to effectively observe the provisions of the Act and the rules made under it. **Protecting Personal Data**: A Data Fiduciary must protect personal data in its possession or under its control, including any processing done by a Data Processor, by	

		taking reasonable security safeguards to prevent personal data breaches. **Intimation of Personal Data Breach**: In the event of a personal data breach, the Data Fiduciary must notify the Data Protection Authority and each affected Data Principal in the prescribed form and manner. **Erasure of Personal Data**: Unless retention is necessary for compliance with the law, a Data Fiduciary must erase and cause its Data Processor to erase personal data upon the withdrawal of consent by the Data Principal or when it is reasonable to assume that the specified purpose is no longer being served. Erase data once purpose for which personal data was taken has been achieved.	The form and manner of intimation of personal data breach to the Board
		Deemed Non-Performance of Specified Purpose: If the Data Principal does not approach the Data Fiduciary for the performance of the specified purpose and does not exercise any rights related to the processing for a prescribed time period, the purpose will be deemed to no longer be served. A Data Principal will be considered as not having approached the Data Fiduciary for the performance of the specified purpose if they have not initiated contact with the Data Fiduciary in person or through electronic or physical communication.	The time period for the specified purpose to be deemed as no longer being served
		Publication Contact Information of DPO: A Data Fiduciary, if applicable, must publish the business contact information of a Data Protection Officer or a person who can answer questions raised by Data Principals about the processing of their personal data. **Grievance Redressal Mechanism**: A Data Fiduciary must establish an effective mechanism to address the grievances of Data Principals.	The manner of publishing the business contact information of a DPO

6.	Processing of personal data of children (Clause 9)	**Verifiable Consent:** A Data Fiduciary must obtain verifiable consent from the parent or lawful guardian of a child or person with a disability before processing their personal data**.** **No Detrimental Effect:** A Data Fiduciary must not undertake any processing of personal data that is likely to cause any detrimental effect on the well-being of a child**.** **No Tracking or Targeted Advertising:** A Data Fiduciary must not undertake tracking or behavioral monitoring of children or targeted advertising directed at children.	The manner of obtaining verifiable consent. The classes of Data Fiduciaries, the purposes of processing of personal data of a child and the conditions relating thereto
7.	Additional Obligations Significant Data Fiduciary (Clause 10)	**Notification of Significant Data Fiduciaries:** The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary based the volume and sensitivity of personal data processed, risk to the rights of Data Principal, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State, and public order. **Obligations of Significant Data Fiduciaries:** Significant Data Fiduciaries must appoint a Data Protection Officer, who will represent the Significant Data Fiduciary, be based in India, be responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary and be the point of contact for the grievance redressal mechanism under the provisions of the Act. They must also appoint an independent data auditor to carry out data audit and	The other matters comprising the process of Data Protection Impact

		undertake periodic Data Protection Impact Assessment, periodic audit, and other measures consistent with the provisions of the Act as may be prescribed.	Assessment. the other measures that the Significant Data Fiduciary shall undertake
8	Rights of data principal (Clause 11,12,13,14)	**Right to Obtain Information:** The Data Principal has the right to obtain following information from the Data Fiduciary on making a request in the prescribed form: a summary of the personal data being processed, and the processing activities undertaken by the Data Fiduciary. The identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared, along with a description of the shared personal data. Any other information related to the personal data and its processing as prescribed. **Right to Correction, Completion, and Updating:** A Data Principal has the right to correction, completion, and updating of their personal data. **Obligations of Data Fiduciary:** Upon receiving a request for correction, completion, or updating from a Data Principal, the Data Fiduciary must correct inaccurate or misleading personal data, complete incomplete personal data, and update the personal data.	The manner in which a Data Principal shall make a request to the Data Fiduciary to obtain information and any other information related to the personal data of such Data Principal

		Right to Erasure: A Data Principal has the right to request erasure of their personal data in a manner prescribed by the Data Fiduciary. Upon receipt of such a request, the Data Fiduciary must erase the personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force. **Right to Grievance Redressal**: Data Principals have the right to register a grievance with the Data Fiduciary or Consent Manager regarding any act or omission related to the performance of their obligations in relation to the personal data of the Data Principal or the exercise of the Data Principal's rights. **Response to Grievances**: The Data Fiduciary or Consent Manager must respond to the grievances within the prescribed period from the date of receipt. The Data Principal must exhaust the opportunity of redressing their grievance under this section before approaching the Board. **Right to Nominate:** Data Principals have the right to nominate any other individual, in a manner prescribed, who will exercise their rights in the event of their death or incapacity.	The manner in which a Data Principal shall make a request to the Data Fiduciary for erasure of her personal data The period within which the Data Fiduciary shall respond to any grievances The manner of nomination of any other individual by the Data Principal

9.	Duties of Data Principal (Clause 15)	**Compliance with Applicable Laws**: The Data Principal must comply with the provisions of all applicable laws while exercising their rights under the provisions of the Act. **No Impersonation**: The Data Principal must ensure not to impersonate another person while providing their personal data for a specified purpose. **No Suppression of Material Information**: The Data Principal must ensure not to suppress any material information while providing their personal data for any document, unique identifier, proof of identity, or proof of address issued by the State or any of its instrumentalities. **No False or Frivolous Grievances**: The Data Principal must ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board. **Furnishing Verifiably Authentic Information**: The Data Principal must furnish only such information as is verifiably authentic while exercising the right to correction or erasure under the provisions of the Act or the rules made under it.	
10.	Processing data outside India (Clause 16)	The Central Government has the authority to notify countries or territories to which the transfer of personal data by a Data Fiduciary for processing is restricted. This section does not limit the applicability of any existing laws in India that provide a higher degree of protection or restrictions on the transfer of personal data by a Data Fiduciary outside India.	
11.	Exemption (Clause 17)	Data fiduciary is exempted from certain obligations (except for being responsible for its data processor and taking reasonable security safeguards), such as notice and consent requirements for certain specified circumstances including	

		(i) where processing of personal data is necessary for enforcing any legal right or claim; (ii) 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 function or regulatory or supervisory function,; where such processing is necessary for the performance of such function; (iii) where personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; (iv) where the 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; (v) for processing necessary for a merger/amalgamation or similar arrangement as approved by a court or tribunal or other authority competent; and (vi) for ascertaining the financial situation of a person who has defaulted on a loan or advance given by a financial institution.	
10.	Penalties (Schedule)	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data – Upto INR 250 crore Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach – Upto INR 200 crore Breach in observance of additional obligations in relation to children – Upto INR 200 crores Breach in observance of additional obligations of Significant Data Fiduciary – Upto INR 150 crores	

		Breach in observance of the duties by Data Principal – Upto INR 10,000 Breach of any other provision of this Act or the rules – Upto INR 50 crores	

CONCLUSION

As companies embark on the journey to align with India's new data protection law, several critical actionable items demand attention. First and foremost, a transparent and user-friendly consent process must be instituted, providing users with clear information on data processing, withdrawal mechanisms, and avenues for grievance redressal. Embracing data minimization principles is imperative, ensuring that only necessary personal data is collected and promptly erased when no longer required. To fortify their systems, companies should implement legally compliant measures, safeguarding against breaches and guaranteeing the accuracy and completeness of data. Essential to this process is the establishment of mandatory contracts with Data Processors, guaranteeing secure data handling. Further, the appointment of a Data Protection Officer and a registered Consent Manager becomes crucial, with the former mandatory for significant Data Fiduciaries. Finally, a robust grievance redressal mechanism must be established, providing a channel for users to address concerns and ensuring a resilient foundation for data protection in the evolving digital landscape.