Checklist for Digital Personal Data Protection (DPDP) Act, 2023

Readiness Review / Assessment Checklist

Areas	**Sub Areas**	**Steps**
Consent	Review existing Data Practices	• Conduct a comprehensive assessment of existing policies & processes with regard to where the data is collected, processed and stored. • Evaluate the organisational need at both the technical and process levels for consent.
	Transparent privacy notice	• Create a clear & transparent privacy notice that clearly outlines what data is collected, why it is collected, how it is used and with whom it will be shared, so that users make an informed decision. • Ensure that the notice is available in multiple languages, as applicable
	Privacy considerations	• Integrate privacy considerations into the design of products and services right from their conceptualisation. • Design user-friendly interfaces like checkboxes and sliders to facilitate user choice for consent. • Incorporate age verification for children (age < 18) and parental consent, as applicable
	Options	• Obtain consent clearly and freely. • Provide granular consent options for users. • Ensure that consent revocation is easy and straightforward.
	Consent managers	• Establish a unified process for dealing with consent managers.
	Cookies	• Ensure that websites have a cookie consent banner that clearly informs users about the use of cookies. • Cookies shall only be allowed after the user has provided their consent for the same. • Consent checkboxes must not be pre-checked. • The website shall allow users to permit only strictly necessary cookies. • Inform users that the website (or any third-party service used by the website) uses cookies • Clearly state which action will signify consent and ensure it is sufficiently conspicuous to make it noticeable • Link to a cookie policy or make details of cookies' purposes, usage and related third-party activities available to the user • Specify the period of validity of cookies or mention the expiry period. • Websites should include an easy-to-use opt-out mechanism that allows users to withdraw their consent and manage their cookie preferences. • The use of cookies should be limited only to purposes essential for the website's proper functioning. Using cookies for unnecessary tracking or data collection must be avoided.
Privacy notice	Data Collection, purpose & legitimate use	• List what data is collected, its type and category • State why data is being collected and the purpose for which it will be used • State definition of legitimate use • Define Retention period
	Data sharing and transfer	• Who are the Data Recipients – e.g., third party, vendors • Are there any cross-border transfers, state details if yes
	Data principal rights	• Establish what are data principal rights and mechanisms • Define process for making complaints to the board
	Contact details of the privacy office/point of contact	• State Data Privacy Officer (DPO) or data privacy office contact details

Areas	Sub Areas	Steps
	Data protection measures	• Define measures for notification of any breaches • Define details of security safeguards in place
Data principal rights	Policy	• Develop clear and documented policies and procedures that outline how the organisation will handle data principal requests, including processes for verifying identity, responding within specified timeframes and maintaining request records
	Update notice	• Review and update privacy notices or policies to include clear information about data subject rights, how they may be exercised and the organisation's contact details for such requests.
	Communication channels	• Establish dedicated communication channels, such as email addresses or online forms, through which data principals can submit requests and inquiries regarding their data rights.
	Technology	• Use tools for data inventories to understand what personal data they collect, where it is stored and how it is processed.
	Data Retention	• Understand data retention and deletion requirements for the concerned sector or organisation so that even if a data principal asks for data erasure, the organisation has a valid reason to retain the data.
Breach notification	Policy	• Define what constitutes a personal data breach • Define an internal breach reporting procedure • Define process to assess the impact of any personal data breach – e.g., number of data principals affected. • Define process to notify the board and data principals in a timely manner.
	Detection and identification	• Process that detects a data privacy breach has occurred. • Define breach monitoring systems and processes to identify if a breach is a security or data privacy breach.
	Assessment	• Conduct a thorough assessment of the breach to understand its extent and impact. • Determine the types of data that were compromised, potential risks to affected individuals and technical details of the breach.
	Notification	• Process to notify affected individuals, customers, partners, regulatory authorities and law enforcement agencies, in a timely and transparent manner. • Establish a communication plan to keep stakeholders informed about the breach, its impact and the steps being taken to address it.
	Remediation	• Define plan for corrective actions to address vulnerabilities or weaknesses that allowed the breach to occur. • Process for implementation of new security measures, as per identified weaknesses that allowed the breach
	Continuous monitoring	• Define process for continuous monitoring of the security posture to prevent future breaches • Define and update security strategies as needed. • Develop comprehensive plan for stakeholder training (employees, third parties, vendors etc.)

Areas	Sub Areas	Steps
Data Privacy Office (DPO)	DPO Requirements, Scope & Governance	• Define process for appointment of DPO (should be based in India), who should report to the board of directors or a similar governing body. • Ensure that DPO is the point of contact for the grievance redressal mechanism. (A significant data fiduciary would need a fulltime DPO Other data fiduciaries can voluntarily have one, depending on the nature of the data)
	Data Privacy Organization	• Define the composition of the DPO team, consisting of data privacy coordinators and data owners from different functions • Define roles and responsibilities, metrics and key performance indicators (KPIs). • Align with functions such as risk, legal and cyber • Ensure that processes are established so that DPO can operate in an independent and transparent manner, ensuring compliance and reporting to the board of directors or an equivalent level
Data Retention	Data Categorisation	• Categorise data that the organisation collects and processes (financial records, employee data, marketing etc.). • Understand legal and regulatory requirements with respect to each category. • Assess business needs and analyse business use. • Develop retention policies for each category – involve legal and compliance in this process. • Establish internal & external communication process • Establish process for effective documentation of the retention period and related information such as data categories, data ownership and basis of retention.
Third-party transfers	Contractual Agreements	• Establish clear and robust contractual agreements with data processors. • State data privacy obligations, security measures and compliance with the DPDP Act.
	Data mapping and inventory	• Conduct a thorough data mapping and inventory exercise to identify all data flows, including identification of data processors.
	Data principal rights	• Ensure data processors cease processing when consent is withdrawn by the data principal. • Ensure erasure of personal data by data processor post completion of specified purpose.
	Data security	• Implement robust security measures to protect personal data during transfers and ensure data processors implement adequate controls as well
	Periodic checks and reviews	• Conduct periodic reviews and checks on the data processor's environment to ensure personal data processing is aligned with the DPDP Act.
Children's personal data	Protection of Data	• Identify minors (Age < 18) - Age of the user of the product or service should be captured to identify if the user is below 18 years • Maintain easily accessible and understandable privacy policies that outline how children's data is collected, used and shared (e.g., is the privacy notice customised to state that children's personal data might be collected?) • Establish process to obtain verifiable parental or guardian consent before collecting any personal data from children and offer parents the ability to review, modify or delete their child's data.

Areas	Sub Areas	Steps
		• Perform a data protection impact assessment (DPIA) to assess risk to children’s data processing. • Identify and address high-risk scenarios, e.g., tracking, behavioural monitoring or targeted advertising using children’s data. • Establish process to incorporate privacy by design principles into development of digital products and services for children. • Define process to implement robust security measures to protect children’s data from unauthorised access or breaches