Privacy Pillar

DPDP Act, 2023 – Compliance Kit

Comprehensive Checklist for Readiness

This kit provides a complete framework for assessing compliance with the Digital Personal Data Protection Act, 2023 across Business operations.

Kit Components:☒- DPDP Act, 2023 Compliance Checklist

Domain	Applicable Privacy Principle	Relevant Provision (Digital Personal Data Protection Act, 2023)	Relevant Provision (Digital Personal Data Protection Rules, 2025)	Question	Response (Yes/No)	Compliance Status (Compliant/Partially Compliant/Not Compliant/Not Applicable)	Detailed Comments
Lawful Processing	Lawfulness Transparency	Section 4(1)	N/A	Has the organization identified and documented a lawful purpose for undertaking every processing activity that involves personal data corresponding to data principals?			
Lawful Processing	Lawfulness	Section 4(2)	N/A	Has the organization assessed and documented that the identified processing purpose for undertaking the processing activity is not expressly prohibited by any applicable law?			
Lawful Processing	Lawfulness	Section 4(1)(a)	Rule 3(b)	Has the organization incorporated appropriate mechanisms in place to obtain valid, specific, and informed consent from data principals prior to processing their data?			
Lawful Processing	Lawfulness Transparency	Section 4(1)(b), Section 7	Rule 5	Has the organization documented the specific legitimate use relied upon and communicated such use to data principals, in case the lawful basis for processing personal data is legitimate use?			
Lawful Processing	Purpose Limitation	Section 4(1)	Rule 3(b)	Has the organization incorporated appropriate mechanisms in place to ensure that the personal data processed is strictly limited to the defined purposes of undertaking the processing activities?			
Lawful Processing	Transparency Purpose Limitation	Section 4(1)	N/A	Has the organization documented and incorporated an appropriate process to identify change in purposes of processing personal data and, whether a change in purpose requires a fresh consent to be obtained from the data principal or a revision in the lawful basis before initiating such a processing activity?			
Notice	Transparency Lawfulness	Section 5 (1)	Rule 3 (a)	Does the organization present a Privacy Notice to the data principals prior to or at the time of obtaining their consent for processing their personal data, in a form that is independently understandable?			
Notice	Transparency	Section 5(1)(i)	Rule 3(b)(i)	Does the organization ensure that such Privacy Notice clearly specifies the itemized categories of personal data proposed to be processed through the processing activities undertaken?			
Notice	Transparency	Section 5(1)	Rule 3(b)	Does the organization ensure that such Privacy Notice is drafted in clear and plain language that enables the data principals to provide their specific and informed consent?			
Notice	Purpose Limitation Transparency	Section 5(1)(i)	Rule 3(b)(ii)	Does the organization ensure that such Privacy Notice clearly states the specific purpose(s) of undertaking the processing of personal data corresponding to data principals, the goods, services, or uses enabled by such processing?			
Notice	Transparency	Section 5(1)(ii)	Rule 3(c)(ii)	Does the organization ensure that such Privacy Notice clearly describes the mechanisms available for Data Principals to exercise their rights under the DPDPA, 2023?			
Notice	Transparency	Section 5(1)(iii)	Rule 3(c)(iii)	Does the organization ensure that such Privacy Notice clearly describes the process for filing a complaint to the Data Protection Board of India?			
Notice	Transparency Lawful Basis	Section 5(1)	Rule 3(c)(i)	Does the organization ensure that such Privacy Notice communicates a direct and easily accessible mechanism to withdraw consent to the data principals, with the similar ease as comparable to providing their consent?			
Consent	Lawfulness Transparency	Section 6(1)	Rule 3(b)	Has the organization incorporated appropriate mechanism in place to ensure that the consent obtained from data principals to process their personal data is free, specific, informed, unconditional and unambiguous, through a clear affirmative action, and limited to personal data necessary for the specified purpose?			
Consent	Purpose Limitation Data Minimization Lawfulness	Section 6(1)	Rule 3(b)(ii)	Has the organization incorporated appropriate mechanism in place to ensure that consent obtained is not bundled for undertaking processing activities or data categories that are not necessary for the specified purpose?			
Consent	Lawfulness	Section 6(4)	Rule 3(c)(i)	Has the organization incorporated appropriate mechanism in place to enable the Data Principal to withdraw consent at any time, and is such withdrawal operationally effective and as easy as obtaining consent from data principals?			
Consent	Accountability	Section 6(6)	N/A	Upon withdrawal of consent, has the organization incorporated appropriate mechanisms in place to cease processing within a reasonable time and ensure that its Data Processors also cease processing, unless otherwise permitted by law?			
Consent	Accountability	Section 6(10)	N/A	Does the organization demonstrate and prove, through records and logs, that valid consent was obtained in accordance with the Act and Rules?			
Legitimate Use	Lawfulness	Section 7(a)	Rule 8(1)	In case personal data corresponding to data principals is processed based on voluntary provision by the data principals, is such processing strictly limited to the specified purpose and stopped once the data principal indicate that they no longer require the service or do not consent?			
Legitimate Use	Lawfulness	Section 7(b)	Rule 5	In case the organization is the State or its instrumentality, is personal data processed for subsidies, benefits, services, licenses or permits strictly in accordance with Rule 5 and applicable law/policy?			
Legitimate Use	Lawfulness	Section 7(c)–(e)	N/A	In case the personal data is processed for State functions, legal obligations, or compliance with judicial or regulatory orders, is such processing clearly traceable to a valid legal mandate and limited to what is required?			
Legitimate Use	Lawfulness	Section 7(f)–(i)	N/A	In case the personal data is processed for medical emergencies, public health situations, disasters, or employment-related purposes, is such processing necessary, proportionate, and restricted to the relevant context?			
Obligations of Fiduciary	Integrity Confidentiality Accountability	Section 8(4)	Rule 6(1)(g)	Has the organization implemented reasonable technical and organizational measures to ensure effective observance of the DPDP Act?			
Obligations of Fiduciary	Integrity Confidentiality Accountability	Section 8(5)	N/A	Has the organization conducted regular security audits and risk assessments to identify and mitigate vulnerabilities?			
Obligations of Fiduciary	Accuracy	Section 8(3)	N/A	Has the organization incorporated an appropriate mechanism to ensure the completeness, accuracy, and consistency of personal data, especially when it is used to make a decision affecting the data principal or is disclosed to another data fiduciary?			
Obligations of Fiduciary	Storage Limitation	Section 8(7)	Rule 8	Has the organization established and documented a clear data retention schedule that ensures that personal data processed therein is retained only as long as necessary for its specified purpose?			
Obligations of Fiduciary	Storage Limitation	Section 8(7)	Rule 8(2)	Has the organization incorporated a mechanism to notify the data principal at least 48 hours before their personal data is scheduled for erasure, as required by the law?			
Obligations of Fiduciary	Integrity Confidentiality Accountability	Section 8(6)	Rule 7	Has the organization documented and incorporated a data breach response plan to notify the Data Protection Board of India (DPBI) and all affected data principals in the event of a personal data breach?			
Obligations of Fiduciary	Accountability	Section 8(6)	N/A	Has the organization documented a register to record all data breaches and security incidents, that shall be maintained as well?			
Obligations of Fiduciary	Accountability	Section 8(2)	Rule 6(1)(f)	Does the organization ensure that a valid contract is in place outlining clear data processing obligations therein, with every data processor that the organization employs, to process personal data on behalf of the organization?			
Obligations of Fiduciary	Storage Limitation Accountability	Section 8(7)	Rule 8(3)	Does the organization have pertinent controls implemented to ensure that its outsourced data processors erase any accessible personal data within the required timeline?			
Obligations of Fiduciary	Accountability Transparency	Section 8(9)	Rule 9	Does the organisation ensure that it prominently publishes the contact details of the Data Protection Officer or the person authorized on behalf of the organization to respond to queries on the processing of personal data through its website or application?			
Processing of Children's Data	Lawfulness	Section 9(1)	Rule 10(1)	Does organisation obtain verifiable consent from a parent or lawful guardian before processing any personal data of a child (any individual below the age of 18 years)?			
Processing of Children's Data	Fairness	Section 9(3)	N/A	Does organisation implement appropriate controls in place to prevent the tracking or behavioral monitoring of children?			
Processing of Children's Data	Purpose Limitation Data Minimization	Section 9	N/A	Does the organisation incorporate appropriate measures in place to ensure that the personal data corresponding to children is collected and processed only to the extent necessary for the specified purpose?			
Additional Obligations of Significant Data Fiduciary	Accountability	Section 10(2)(a)	N/A	In case the organization is designated as a Significant Data Fiduciary (SDF) by way of the Central Government notification, has it appointed a Data Protection Officer?			

Additional Obligations of Significant Data Fiduciary	Accountability	Section 10(2)(c)	Rule 13(1)	In case the organization is designated as a Significant Data Fiduciary (SDF) by way of the Central Government notification, has it conducted periodic Data Protection Impact Assessments (DPIAs) to assess and manage risks posed to the rights of Data Principals?			
Additional Obligations of Significant Data Fiduciary	Accountability	Section 10 (2) (b)	Rule 13 (2)	In case the organization is designated as a Significant Data Fiduciary (SDF) by way of the Central Government notification, has it appointed an Independent Data Auditor to carry out a data audit of its systems and compliance?			
Right to Access	Transparency Accountability	Section 11	Rule 14 (1)	Does the organization have a clear and easily accessible process for data principals to request and obtain a summary of their personal data processed therein?			
Right to Correction	Transparency Accountability	Section 12	Rule 14 (1) (a)	Does the organization provide a clear and easily accessible mechanism for data principals to request the correction, completion, or updating of their personal data processed therein?			
Right to Erasure	Transparency Accountability	Section 12	Rule 14 (1) (a)	Does the organization provide a clear and easily accessible mechanism for data principals to request the erasure of their personal data processed therein?			
Right to Nominate	Transparency Accountability	Section 13	Rule 14 (4)	Does the organization provide a clear and easily accessible mechanism for data principals to exercise their right to nominate another individual who shall exercise their rights in the event of death or incapacity of a data principal?			
Right to Grievance Redressal	Transparency Accountability	Section 14	Rule 14 (3)	Does the organization provide a clear and easily accessible grievance redressal mechanism in place that allows data principals' grievances to be addressed by the Data Protection Officer or a Grievance Officer?			
Data Principal Rights	Transparency Accountability	Section 8 (1)	Rule 8(3)	Does the organization maintain records of all data principal requests received and their resolution to ensure accountability?			
Data Principal Rights	Transparency Accountability	Section 8 (1)	Rule 14 (3)	Does the organization address and manage such requests within a reasonable and defined timeline as under the regulation?			
Notice	Transparency	Section 5	Rule 3 (c) (ii)	Does the organization present a Privacy Notice to the data principals that clearly explains the mechanism to exercise their rights, such as the right to access, correct, and erase their personal data?			
Cross Border	Lawfulness Accountability	Section 16	Rule 15	Has the organization implemented appropriate controls to monitor and prevent transfers of personal data to any country or territory that may be restricted by notifications issued by the Central Government?			
Cross Border	Integrity Confidentiality Accountability	Section 16	Rule 15	Has the organization implemented adequate safeguards, including encryption and appropriate contractual obligations (such as data transfer agreements), to protect the personal data that could be involved in international data transfers?			
Technical and Organizational Measures	Accountability Integrity Confidentiality	Section 8(4)	N/A	Has the organization conducted data privacy training sessions for all employees and contractors who handle personal data?			