DPDP Act 2023 Compliance Template

Complete Implementation Guide for Digital Personal Data Protection Act | Prepared by TCSA

About This Template

What's Included: 47-point compliance checklist, data mapping framework, consent management templates, Data Principal Rights (DPR) processes, and sample privacy policy clauses.

Who This Is For: Indian startups and SMBs handling personal data who need to comply with DPDP Act 2023.

Enforcement: DPDP Act came into force in August 2023. Penalties up to ₹250 crores for non-compliance.

Section 1: DPDP Act Compliance Checklist (47 Requirements)

#	Requirement	DPDP Reference	Status	Priority	Notes
1	Obtain valid consent before processing personal data	Section 6	□	High	
2	Ensure consent is free, specific, informed, unconditional, and unambiguous	Section 6(1)	□	High	
3	Provide clear notice in English/22 scheduled languages	Section 5	□	High	
4	Identify lawful basis for processing (consent or legitimate use)	Section 7	□	High	
5	Process data only for specified purpose	Section 4(a)	□	High	
6	Limit data collection to what's necessary	Section 4(b)	□	High	
7	Ensure data accuracy and completeness	Section 4(c)	□	Medium	
8	Implement data retention and deletion policies	Section 4(d)	□	High	
9	Implement reasonable security safeguards	Section 8	□	High	
10	Report data breaches to Data Protection Board within 72 hours	Section 8(6)	□	High	
11	Implement consent withdrawal mechanism	Section 6(4)	□	High	
12	Make consent withdrawal as easy as giving consent	Section 6(5)	□	High	
13	Maintain consent records and audit trail	Section 6	□	High	
14	Obtain separate consent for different purposes	Section 6(2)	□	High	
15	Obtain verifiable parental consent for children under 18	Section 9	□	High	
16	Provide mechanism for data access requests	Section 11(1)	□	High	
17	Provide mechanism for data correction requests	Section 11(2)	□	High	
18	Provide mechanism for data erasure requests	Section 11(3)	□	High	
19	Provide mechanism for grievance redressal	Section 11(4)	□	High	
20	Respond to DPR requests within prescribed timeline	Section 11	□	High	
21	Appoint Data Protection Officer (if Significant Data Fiduciary)	Section 10(1)(a)	□	Medium	

#	Requirement	DPDP Reference	Status	Priority	Notes
22	Publish contact details of Data Protection Officer	Section 10(1)(a)	☐	**Medium**	
23	Execute Data Processing Agreements (DPA) with processors	Section 8(4)	☐	**High**	
24	Ensure processors implement adequate security measures	Section 8(5)	☐	**High**	
25	Conduct vendor due diligence for data processors	Section 8	☐	**High**	
26	Monitor processor compliance with DPA terms	Section 8	☐	**Medium**	
27	Identify countries for cross-border data transfers	Section 16	☐	**High**	
28	Ensure transfers only to approved countries (when notified)	Section 16	☐	**High**	
29	Implement Standard Contractual Clauses (SCCs) for transfers	Section 16	☐	**Medium**	
30	Implement Privacy by Design in product development	Section 8	☐	**Medium**	
31	Conduct Data Protection Impact Assessments (DPIA)	Section 10(1)(b)	☐	**Medium**	
32	Conduct periodic audits of data processing activities	Section 10(1)(c)	☐	**Medium**	
33	Create and publish Privacy Policy	Section 5	☐	**High**	
34	Maintain Record of Processing Activities (RoPA)	Section 8	☐	**High**	
35	Document data retention and deletion procedures	Section 4(d)	☐	**High**	
36	Create data breach response plan	Section 8(6)	☐	**High**	
37	Document consent collection mechanisms	Section 6	☐	**High**	
38	Implement encryption for data at rest and in transit	Section 8	☐	**High**	
39	Implement access controls and authentication	Section 8	☐	**High**	
40	Implement logging and monitoring systems	Section 8	☐	**High**	
41	Conduct employee training on DPDP compliance	Section 8	☐	**Medium**	
42	Implement data minimization in systems	Section 4(b)	☐	**Medium**	

#	Requirement	DPDP Reference	Status	Priority	Notes
43	Implement automated data deletion workflows	Section 4(d)	□	**Medium**	
44	Designate internal DPDP compliance owner	Section 8	□	**High**	
45	Establish data governance framework	Section 8	□	**Medium**	
46	Conduct regular compliance reviews	Section 8	□	**Medium**	
47	Maintain evidence of compliance for audits	Section 8	□	**High**	

Section 2: Data Mapping Template

Map all personal data your organization processes. This is the foundation of DPDP compliance.

Data Category	Data Elements	Purpose	Lawful Basis	Storage Location	Retention	3rd Parties
Customer Data	Name, Email, Phone	Service delivery	Consent	AWS Mumbai	3 years	Payment gateway
Employee Data	Name, PAN, Aadhaar	HR management	Legitimate use	On-premise	7 years	Payroll vendor
Marketing Data	Email, preferences	Marketing	Consent	AWS Mumbai	Until withdrawal	Email service
Add your organization's data categories...						

Section 3: Consent Management Framework

Consent Notice Template (Section 5 & 6 Compliance)

What data we collect: [List specific data elements: name, email, phone, etc.]

Why we collect it: [Specific purpose: to process your order, send newsletters, etc.]

Who we share it with: [List third parties: payment processors, shipping partners, etc.]

How long we keep it: [Retention period: 3 years after last transaction, etc.]

Your rights: You can access, correct, or delete your data anytime by contacting [email/phone].

How to withdraw consent: Click "Manage Preferences" in any email or contact us at [email].

☐ **I consent to the above** (Checkbox must be unchecked by default)

Consent Requirements Checklist

Requirement	Implementation	Status
Consent must be freely given (no coercion)	Don't make service conditional on consent for non-essential processing	☐
Consent must be specific (purpose-bound)	Separate checkboxes for different purposes (marketing vs service delivery)	☐
Consent must be informed (clear notice)	Provide notice in plain language before collecting consent	☐
Consent must be unambiguous (affirmative action)	Use opt-in checkboxes (unchecked by default), not pre-ticked boxes	☐
Consent must be unconditional (no bundling)	Don't bundle consent for multiple unrelated purposes	☐
Withdrawal must be as easy as giving consent	One-click unsubscribe, preference center, or email/phone contact	☐
Maintain consent records	Log: who consented, when, for what purpose, IP address, consent text shown	☐

Section 4: Data Principal Rights (DPR) Process

DPR Request Handling Workflow

Request Type	What to Do	Timeline	Response Template	Status
Access Request (Section 11.1)	Provide copy of all personal data you hold about the requester	Within 30 days	"We are processing the following data about you: [list]. Attached is a copy."	□
Correction Request (Section 11.2)	Verify identity, update inaccurate data, notify third parties if shared	Within 30 days	"We have corrected your [field] from [old] to [new]."	□
Erasure Request (Section 11.3)	Delete data unless legal obligation to retain (e.g., tax records for 7 years)	Within 30 days	"We have deleted your data. Note: [any exceptions, e.g., tax records retained for 7 years]."	□
Grievance (Section 11.4)	Acknowledge within 24 hours, investigate, resolve within 30 days	Within 30 days	"We have investigated your concern and [resolution]."	□

DPR Request Form Template

Request Type: □ Access my data □ Correct my data □ Delete my data □ Grievance

Your Name: _____

Email/Phone used for our service: _____

Details of your request: _____

Identity Verification: Please provide [Aadhaar/PAN/other ID] to verify your identity.

Submit to: [dpo@yourcompany.com] or [phone number]

Section 5: Sample Privacy Policy Clauses

1. Data We Collect

"We collect the following personal data: [name, email, phone, address, payment details, etc.]. We collect this data when you [sign up, make a purchase, contact us, etc.]."

2. How We Use Your Data

"We use your personal data for the following purposes:

• To provide our services to you (lawful basis: consent)

• To process payments (lawful basis: contract performance)

• To send you marketing communications (lawful basis: consent - you can opt out anytime)

• To comply with legal obligations (lawful basis: legal requirement)"

3. Data Sharing

"We share your data with the following third parties:

• Payment processors: [Razorpay/Stripe] for payment processing

• Cloud providers: [AWS/Google Cloud] for data storage

• Marketing tools: [Mailchimp/SendGrid] for email communications (only if you consented)

We do not sell your personal data to anyone."

4. Data Retention

"We retain your personal data for:

• Customer data: 3 years after last transaction

• Marketing data: Until you withdraw consent

• Financial records: 7 years (legal requirement)

After this period, we securely delete your data."

5. Your Rights

"Under the DPDP Act 2023, you have the right to:

• Access your personal data

• Correct inaccurate data

• Request deletion of your data

• Withdraw consent anytime

• File a grievance if you're unhappy with how we handle your data

To exercise these rights, contact us at [email/phone]."

6. Data Security

"We implement industry-standard security measures including:

• Encryption of data in transit and at rest

• Access controls and authentication

• Regular security audits

• Employee training on data protection

In case of a data breach, we will notify you and the Data Protection Board within 72 hours."

7. Contact Us

"For any questions about this Privacy Policy or to exercise your rights, contact:

Data Protection Officer: [Name]

Email: [dpo@yourcompany.com]

Phone: [+91-XXXXXXXXXX]

Address: [Your registered office address]"
