

# Privacy Policy Analysis Against DPDP Act, 2023

## Key Findings

- Lack of Explicit Consent Mechanism** – The policy does not clearly describe how consent is obtained, stored, or withdrawn, as required under [Section 6 of the DPDP Act](#).
- Insufficient Notice Requirements** – The policy does not provide an itemized description of personal data collected or the specific purposes of processing, as mandated by [Rule 3 of the DPDP Rules](#).
- No Mention of Data Principal Rights** – The policy does not explicitly inform users of their rights (access, correction, erasure, grievance redressal) under [Sections 11-14 of the DPDP Act](#).
- No Data Breach Notification Process** – The policy does not outline procedures for notifying users in case of a data breach, as required under [Section 8\(2\) of the DPDP Act](#).
- No Data Retention & Erasure Policy** – The policy does not specify retention periods or conditions for data erasure, violating [Section 8\(3\) of the DPDP Act](#).
- No Grievance Redressal Mechanism** – The policy does not provide a clear process for users to raise complaints, as mandated by [Section 13 of the DPDP Act](#).

## Compliance Gaps

Privacy Policy Section	DPDP Act Requirement	Gap Identified
"What we collect"	<a href="#">Rule 3(b)(i)</a> – Itemized description of personal data	Lists broad categories but lacks specificity on exact data fields collected.
"What we do with the information"	<a href="#">Section 4(2)</a> – Purpose limitation	Does not clearly link each data type to a specific lawful purpose.
"Controlling your personal information"	<a href="#">Section 11-14</a> – Data Principal rights	No explicit mention of rights to access, correct, or erase data.
"Security"	<a href="#">Section 8(1)</a> – Security safeguards	Lacks details on encryption, access controls, or breach response.
No Data Retention Policy	<a href="#">Section 8(3)</a> – Data erasure	Does not specify retention periods or conditions for deletion.
No Grievance Officer	<a href="#">Section 13</a> – Grievance redressal	No designated contact for complaints.

delivery).

### 3. User Rights (Non-Compliant)

- **Issue:** No mention of rights under [Sections 11-14](#).
- **Fix:** Add a dedicated "Your Rights" section with steps to request data access/correction.

### 4. Security Measures (Insufficient)

- **Issue:** Lacks technical safeguards (encryption, access logs) per [Section 8\(1\)](#).
- **Fix:** Specify **encryption standards, audit logs, and breach response protocols**.

### 5. Data Retention (Missing)

- **Issue:** No retention policy as per [Section 8\(3\)](#).
- **Fix:** Define **retention periods** (e.g., 1 year for inactive users) and auto-deletion rules.

### 6. Grievance Mechanism (Absent)

- **Issue:** No process for complaints under [Section 13](#).
  - **Fix:** Appoint a **DPO** and provide a **complaint form** with resolution timelines.
- 

## Conclusion

The current privacy policy **does not fully comply** with the DPDP Act, particularly in:

- ✓ **Consent & Notice**
- ✓ **User Rights**
- ✓ **Data Security & Breach Response**
- ✓ **Retention & Erasure**
- ✓ **Grievance Redressal**

#### Immediate Action Required:

- **Redraft the policy** to include all DPDP-mandated disclosures.
- **Implement a consent management system.**
- **Publish a data retention & erasure policy.**
- **Appoint a DPO/grievance officer.**

Would you like a revised privacy policy draft aligned with the DPDP Act? Let me know!