DPDP Biometric Compliance Checklist

This checklist helps organizations align their biometric systems with India’s DPDP Act, 2023. It covers notices, consent, purpose limitation, minimization, retention, cross-border flows, and accountability.

✔■ Compliance Checklist

- Publish clear and plain-language privacy notices at collection points.
- Obtain explicit, revocable consent before collecting biometric data.
- Collect only minimum necessary biometric data (templates, not raw images).
- Define a clear retention schedule and automate deletion when purpose ends.
- Restrict cross-border transfers to approved jurisdictions only.
- Execute Data Processing Agreements (DPAs) with all vendors handling biometrics.
- Encrypt biometric templates at rest and in transit.
- Maintain access logs and deletion logs for audit purposes.
- Appoint a Data Protection Officer (DPO) if processing is large-scale or sensitive.
- Conduct Data Protection Impact Assessments (DPIAs) for new biometric deployments.
- Train employees handling biometric systems on DPDP obligations.

■ Sample Retention Schedule

Data Type	Purpose	Retention Period	Deletion Method	Responsible Team
Fingerprint Template	Employee attendance	90 days post-exit	Secure DB wipe	HR + IT Security
Access Control Logs	Security audit trail	12 months	Log rotation/archive	IT Security
Visitor Biometrics	One-time access	7 days	Auto-purge	Facilities Team