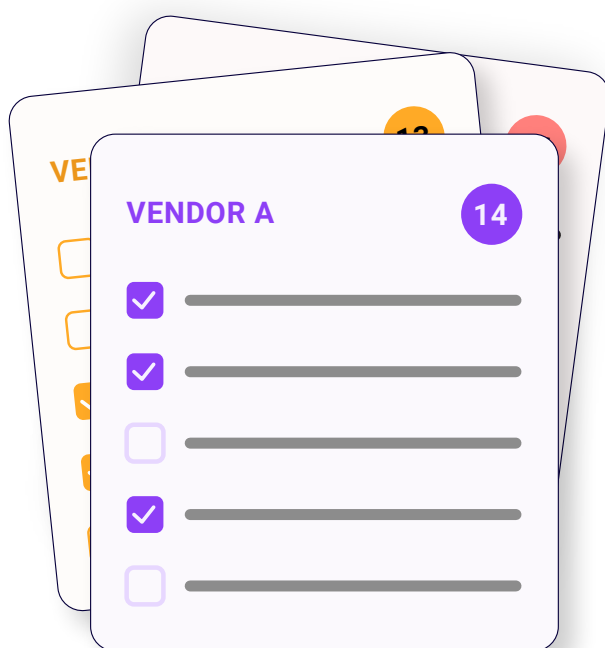


A buyer's practical checklist for

Evaluating a DPDP Compliance Platform

.....

A checklist to evaluate your DPDP compliance vendors feature-by-feature, so you know exactly what you're buying.



Why you need this checklist:

Most DPDP compliance platforms look identical in a sales deck. The differences show up later, during implementation, during an audit, or during a rights request that doesn't reach every system it should.

To help simplify this process, we've created a DPDP Compliance Platform Evaluation Checklist which breaks the platform evaluation down into 16 categories, covering:

- Consent management,
- Rights fulfilment,
- Retention and deletion,
- Data discovery,
- Vendor and risk management,
- Breach response,
- Security,
- Deployment etc.

How to use this framework:

- **Column 1:** Key outcomes your DPDP compliance system must enable
- **Column 2:** Features that help achieve each outcome
- **Column 3:** Space for comments, comparisons, or specific notes

You can print the checklist, use individual sheets for each vendor and score them against the same list. This way, each platform can be evaluated side-by-side and you can compare each vendor's capabilities when presenting or comparing internally.

DPDP Compliance Vendor Evaluation Checklist

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
1. Consent Management		
Multi-channel consent capture	☐ Website ☐ App ☐ API ☐ IVR ☐ WhatsApp/SMS/Email ☐ QR ☐ Branch/field-agent	
Granular, purpose-specific consent	☐ Capabilities for purpose-wise selection ☐ Purpose tagging (mandatory, optional, marketing, servicing, KYC, cross-sell, etc.)	
No-code notice management	☐ No-code notice builder ☐ Version control on notices	
Full consent lifecycle tracking	☐ Update consent state when consent is given/updated/withdrawn/expired/renewed ☐ Expiry reminders	
Automated withdrawal	☐ Purpose-wise withdrawal capabilities ☐ Processing stops automatically ☐ Withdrawal pushed to downstream systems	
Authentication before consent action	☐ Identity verified (OTP, email, or login-based) before consent is given or withdrawn	
Consent Records & Audit Trail	☐ Timestamped record for every action ☐ Records purpose, notice version, language, channel, time ☐ Can't be edited or deleted, even by admins ☐ Shows consent status as of any past date ☐ Records retained even after withdrawal or notice change ☐ Exportable in regulator-accepted formats (PDF/Excel/JSON)	

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
2. Cookie Consent		
Automated cookie scanning	☐ Scans and categorizes all cookies/trackers automatically	
Blocks cookies until consent given	☐ Non-essential cookies stay off until the user consents	
Customizable cookie banner	☐ Banner design matches your brand	
Category-level cookie choice	☐ Choose by category (essential, analytics, marketing) ☐ Change preferences anytime	
Provable cookie consent	☐ Cookie consent logs kept as evidence	
3. Rights Management		
Rights request portal	☐ Self-service portal for access, correction, deletion, grievance requests ☐ Integration with support channels like email/App/WhatsApp	
Authentication before request is processed	☐ Identity verified (OTP, email, or login-based) before a rights request is processed	
Requests tracked to deadline	☐ Tracked against DPDP-mandated response deadlines	
Nominee support	☐ Nominee can act after death or incapacity	
Guardian & representative support	☐ Accepts requests from guardians, parents, or other authorised representatives (e.g. for minors or persons with disabilities)	
Proof of response	☐ Proof generated for every completed request	
4. Data Retention & Deletion		
Rule-based deletion	☐ Event-triggered retention rules (withdrawal, contract end, etc.)	
Regulator-mapped retention	☐ Retention mapped to RBI/SEBI/IRDAI requirements	

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
Automated deletion instructions	☐ Auto-instructs other systems and third parties to delete when a trigger fires	
Automatic deferred deletion	☐ Auto-sets a future deletion date where longer retention is required	
Confirmed deletion	☐ Permanent log of every deletion	
Maker-checker on deletion	☐ Deletion can be gated behind an approval step	
5. Data Discovery & Mapping		
Full data source coverage	☐ Scans structured systems - databases, CRM, core systems ☐ Scans unstructured systems - emails, spreadsheets, cloud drives	
Automatic sensitive-data detection	☐ Auto-classifies personal/sensitive data - no manual tagging	
Live ROPA mapping	☐ Auto-builds ROPA from discovery ☐ Re-scans regularly for new data	
On-premise deployment option	☐ On-premise deployment available	
6. Assessments & Risk Management		
Ready-made assessment templates	☐ Ready-made assessment templates including DPIA and PIA	
Automated assessment triggers	☐ When new vendor, data type, or cross-border transfer needs review	
Risk scoring	☐ Risk scoring capabilities	
Central risk register	☐ Single risk register across the organization	
Mitigation tracking	☐ Mitigation tasks assigned with owner and deadline	
Automated reminders	☐ Capability to auto-send reminders where action is due	

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
Review and approve workflow	☐ Review and approve step before sign-off	
7. Vendor & Third-Party Management		
Vendor registry	☐ Registry of vendors and data shared with each	
Vendor risk assessment	☐ Standard vendor risk-check templates	
Consent-gated data sharing	☐ Blocks data to a vendor if consent isn't in place	
Enforced vendor requests	☐ Sends deletion/correction requests to vendors ☐ Auto-notifies vendors when consent is withdrawn ☐ Captures vendor confirmation	
Contract tracking	☐ DPAs and privacy clauses tracked per vendor	
8. Breach Response		
Affected-customer identification	☐ Structured breach workflow ☐ Auto-categorizes affected individuals	
Timely, compliant notifications	☐ Pre-set templates for the Data Protection Board and affected individuals ☐ Tracks DPDP deadline ☐ System retains time-stamped record of notifications sent	
Breach readiness drills	☐ Supports practice/simulation drills	
9. Legacy Customer Consent (One-Time Notice)		
Multi-channel legacy outreach	☐ App ☐ SMS ☐ WhatsApp ☐ Email ☐ Letter (if no digital contact) ☐ IVR	

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
Response capture	☐ Each response recorded and linked to a consent record	
Bulk notice issuance	☐ Bulk issuance with response tracking	
Automatic channel fallback	☐ Auto-fallback to next channel if one fails	
10. Reach & Accessibility		
Multi-language notice support	☐ Real-time translation of consent notice to regional languages ☐ Language translation according to geo-location	
Low-connectivity support	☐ IVR support ☐ Works on feature phones/weak connectivity	
Children's data handling	☐ Verifiable parental consent ☐ DigiLocker-based age/identity check	
Branch consent	☐ Explicit confirmation step required per customer for assisted consent given at the branch	
Accessibility compliance	☐ Meets accessibility requirements for persons with disabilities	
11. Unified Dashboard & Governance		
Unified cross-module dashboard	☐ Single dashboard across consent, rights, retention, discovery, assessments, breach	
Org-wide risk visibility	☐ Org-wide risk overview	
Role-based access control	☐ Role-based access and permissions	
Change approval workflow	☐ Approval step for critical config changes	
Secured admin access	☐ MFA/SSO for privileged users	

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
12. Deployment, Integration & Implementation		
Flexible deployment	☐ Available on-premise ☐ Available as SaaS	
Minimal data exposure mode	☐ Runs on anonymised IDs and consent status for internal security	
System integration	☐ API/webhook/SDK integration with CBS, LOS, CRM, DBS	
Real-time consent status	☐ Live consent status exposed via API	
No-code business configuration	☐ Configurable without developer involvement	
Fast go-live	☐ Go-live period is short	
Data-blind operation	☐ Platform is blind to your personal data	
13. Data Residency		
On-premise deployment	☐ Can be deployed on-prem, so data never has to leave your environment	
India data residency	☐ Data, records, logs and configuration are all hosted in India	
No indirect data leakage	☐ No metadata/diagnostic data leaves the country	
Default cross-border blocking	☐ Geo-fencing at infra and app level	
14. Security & Certifications		
Recognized certifications	☐ ISO 27001 ☐ ISO 27017 ☐ ISO 27018 ☐ ISO 22301 ☐ SOC 2	
End-to-end encryption	☐ Encrypted at rest and in transit	

Outcome	Feature Checklist (indicative)	Evaluation Notes / Comments
Tight access control	☐ RBAC ☐ MFA/SSO	
Independent security testing	☐ Regular audits and penetration testing	
15. Trustworthiness & Track Record		
Regulatory expertise	☐ RegTech background ☐ Meaningful history in the compliance space	
Proven enterprise scale	☐ Existing enterprise deployments	
16. Ongoing Support		
Regulatory update support	☐ Regulatory updates provided as DPDP Rules evolve	
Post-launch support	☐ Dedicated success manager ☐ Go-live/implementation support	
Committed support SLA	☐ Committed support SLA	

Consentin is an all-in-one DPDP compliance platform for all your privacy compliance needs.



Consent Collect

Collect consent with minimal drop-offs across various channels.



Cookie Consent

Manage cookie consent without slowing down website performance.



Consentin Lens

Discover and map personal data across structured and unstructured systems.



Privacy Centre

Allow customers to manage consent and raise grievances on your platform.



Rights Management

Log, assign, and track every rights request against its SLA.



Retention & Deletion

Automate retention and deletion across internal systems and third-party vendors.



Assessments

Conduct DPIA, PIA and third-party assessments and automate risk management.



Breach Notification

Manage breach response workflows and send breach notifications.

30+ ongoing DPDP implementations

5000 TB of data under discovery

Privacy-first companies have already started using Consentin:





www.consent.in