INTERNAL TEAM WORKSHEET

SDF Likelihood And Readiness Matrix

Assess Significant Data Fiduciary Exposure Under DPDP

USE THIS FOR

Leadership, privacy, security, and legal teams assessing SDF exposure.

Help a business assess SDF exposure signals and prepare for additional obligations without claiming that any unofficial threshold is settled law.

RECOMMENDED WORKFLOW

Complete the worksheet, assign owners, and preserve evidence.

This asset is designed to be shared with internal legal, product, operations, security, and leadership teams.

Important note: Use with current law, official rules, and qualified review for high-risk decisions.

Page 1: Exposure Signals

Score each area as Low, Medium, High, or Unknown.

EXPOSURE AREA	LOW SIGNAL	MEDIUM SIGNAL	HIGH SIGNAL	YOUR RATING	NOTES
Volume of personal data	Small, local dataset	Growing national user base or large customer database	Very large user base, national platform, or high transaction volume		
Sensitivity of data	Basic contact/account data	Financial, employment, location, or identity data in limited scope	Health, biometric, children's, precise location, identity, or financial data at scale		
Risk to Data Principal rights	Low-impact processing	Some profiling or eligibility decisions	Decisions affect jobs, credit, insurance, healthcare, education, housing, essential services, or account access		
Automated decision-making	No automated decisions	Rules or scoring assist human decisions	AI/model-based ranking, scoring, eligibility, fraud, moderation, or profiling with material impact		
Public-order relevance	No public-order impact	Communications or communities with limited public impact	Mass messaging, civic platform, crisis response, public-safety relevance		
Electoral/democracy relevance	No political/civic data	Occasional civic or campaign data	Political profiling, voter targeting, civic influence, public opinion manipulation risk		
Sovereignty/security relevance	No strategic relevance	Regulated-sector dependency	Critical infrastructure, national-scale services, defence/security-adjacent processing		
Processor complexity	Few vendors	Multiple processors and data exports	Complex vendor network, cross-system duplication, hard-to-control downstream copies		
Data breach impact	Limited harm likely	Moderate financial/reputation harm	Material harm to large groups or high-risk individuals		

Page 2: Readiness Baseline

CONTROL AREA	NOT READY	PARTIAL READINESS	STRONG READINESS	CURRENT STATE	OWNER
Processing inventory	No current map	Key systems mapped only	Purpose, data category, legal basis, system, vendor, retention mapped		
Consent records	Scattered or incomplete	Consent captured in main product only	Unified consent records with withdrawal propagation		
Rights workflow	Manual inbox handling	Basic ticket handling	Verified workflow with SLA, vendor action, evidence		
Grievance mechanism	No dedicated process	Support handles privacy complaints	Named grievance route with tracking and escalation		
DPO operating model	No candidate	Privacy owner identified	India-based DPO candidate, authority, board line, contact route		
Data auditor readiness	No audit evidence	Some policies and screenshots	Evidence library, controls, logs, audit owner		
DPIA process	No DPIAs	Informal risk reviews	DPIA template, trigger rules, approvals, mitigations		
Vendor contracts	Old or inconsistent	Key vendors reviewed	Processor clauses for rights, deletion, breach, audit, assistance		
Breach response	No tested plan	Incident plan exists	Tested 72-hour response workflow with roles and templates		
Algorithm governance	No model records	Some model notes	Purpose, data inputs, testing, human review, grievance path		

Page 3: Readiness Decision

Use the pattern, not the exact numeric score.

If Most Exposure Signals Are Low

Recommended action:

- maintain ordinary DPDP readiness
- implement rights and grievance workflows
- keep processing inventory current
- review SDF exposure every 6 months or after major product changes

If Several Exposure Signals Are Medium

Recommended action:

- assign SDF readiness owner
- review vendor contracts
- run one DPIA for highest-risk workflow
- map high-risk processing first
- identify DPO candidate
- brief leadership on potential notification exposure

If Any Exposure Signal Is High

Recommended action:

- treat SDF readiness as a leadership-level workstream
- prepare independent audit evidence
- test rights and breach response workflows
- prepare 90-day remediation plan
- identify DPO operating model
- run DPIAs for high-risk processing
- document algorithmic systems and decision impacts

Page 4: 90-Day Action Plan

TIMEFRAME	ACTION	OUTPUT
Days 1-15	Identify high-volume and high-sensitivity processing	SDF exposure map
Days 1-15	List automated decisions, profiling, scoring, and ranking systems	Algorithm inventory
Days 16-30	Assign privacy owner and DPO candidate	Governance note
Days 16-30	Create leadership escalation path	Board/leadership reporting route
Days 31-45	Complete processing inventory for high-risk systems	Data map
Days 31-45	Review notices, consent flows, and withdrawal paths	Consent gap log
Days 46-60	Review processor contracts for audit, deletion, breach, and rights support	Vendor remediation plan
Days 46-60	Create or update rights request tracker	Rights evidence process
Days 61-75	Run DPIA for highest-risk processing	DPIA report and mitigation plan
Days 61-75	Run breach tabletop exercise	Incident-response evidence
Days 76-90	Build audit evidence folder	SDF readiness pack
Days 76-90	Present risks and remediation to leadership	Readiness decision memo

Page 5: Evidence Pack Checklist

Keep these documents ready if SDF notification or scrutiny arrives.

EVIDENCE ITEM	READY?	LOCATION
Processing inventory	Yes / No	
Consent notices and versions	Yes / No	
Consent logs and withdrawal logs	Yes / No	
Data Principal rights request logs	Yes / No	
Grievance logs	Yes / No	
Data retention schedule	Yes / No	
Vendor/processor list	Yes / No	
Processor contracts and DPAs	Yes / No	
Breach response plan	Yes / No	
Breach tabletop results	Yes / No	
DPIA template	Yes / No	
Completed DPIAs for high-risk processing	Yes / No	
Algorithm or automated-decision inventory	Yes / No	
Security-control evidence	Yes / No	
DPO role description and escalation path	Yes / No	
Audit plan or audit evidence folder	Yes / No	

Footer Disclaimer

This matrix is for readiness planning only. It does not determine whether an organisation is legally a Significant Data Fiduciary. SDF status under DPDP depends on notification by the Central Government and should be reviewed with qualified legal counsel.