GSTRIDE AI

DPDP VENDOR RISK ASSESSMENT · 2026 EDITION

DPDP Vendor Risk Assessment Worksheet.

14 questions to score any workplace AI or productivity intelligence vendor against the Digital Personal Data Protection Act 2023 — designed for India CISOs, DPOs, and Compliance Heads ahead of DPDP Rules notification.

FOR
[Vendor under evaluation]

EVALUATOR
[CISO / DPO / Compliance Head]

EDITION
v1.0 · May 2026

Disclaimer. This worksheet is a procurement aid, not legal or compliance advice. The Digital Personal Data Protection Act 2023 is in force; the implementing DPDP Rules are expected late 2025 / 2026 and the exact notification date should be verified with counsel before any compliance assertion. Penalty exposure under the Act can run up to INR 250 crore per category in the headline tier; per-violation tiers, Schedule 1 carve-outs, and Significant Data Fiduciary designation criteria remain subject to Rules notification — verify with counsel before quoting. gStride is not certified or approved by the Data Protection Board or the Ministry of Electronics and Information Technology; "designed against DPDP categories" describes architecture choices, not regulatory endorsement. gStride does not assert whether it is, or is not, classified as a Significant Data Fiduciary; that designation is pending official criteria.

How to use this worksheet

This is a **14-question worksheet** built for an Indian CISO, DPO, or Compliance Head running diligence on a workplace AI or productivity intelligence vendor against the DPDP Act 2023. It is built to be filled in by the buyer during a vendor demo or written diligence cycle — the rubric, scoring, and verdict bands are all printed on the page itself.

The 14 questions sit inside five blocks. Blocks A through D contribute to the score; Block E is a single halt question that fires the halt verdict on its own.

BLOCK A · 4 QUESTIONS

Consent & Notice. Per-employee consent record, plain-language notice template, withdrawal flow, child / minor carve-out.

BLOCK B · 4 QUESTIONS

DPIA & Risk Management. Inference-layer DPIA, refresh cadence, risk-management framework, 72-hour breach notification path.

BLOCK C · 3 QUESTIONS

Significant Data Fiduciary Obligations. Independent audit, reporting cadence, sensitive- and child-data segregation.

BLOCK D · 2 QUESTIONS

Data Principal Rights & Cross-Border. Rights workflow with statutory SLA, cross-border policy with blacklist support.

BLOCK E · 1 HALT QUESTION

Surveillance Default Posture. Screenshot / keystroke / webcam / mic capture default at install. Score 0 on Q14 fires the halt verdict regardless of total.

How scoring works. Each question in Blocks A through D is scored 0 (fail), 1 (partial), 3 (mostly), or 5 (full). Sum across the 13 scored questions for a total out of 65. The verdict band table translates the total into an action: DPDP-ready (55-65), Gaps to close before Rules notify (35-54), or High-risk — switch needed (< 35). Block E (Q14) is a standalone halt — score 0 there and the verdict is halt regardless of total.

How the gStride reference column works. Each question carries a column showing gStride's posture on that criterion. The column is for reference only — it is not the answer for the vendor you are scoring. The intent is to give the buyer a worked example of what a 5-of-5 answer reads like in writing. gStride's posture is described as designed-with-DPDP-categories-in-mind, deployer-friendly, with consent granular by default and no off-by-default capture. No certification is claimed or implied.

Recommended workflow. One pass per vendor during demo; second pass with the deployer's DPO for Block B and Block E; verdict band reviewed with counsel before the contract conversation. Re-validate at DPDP Rules notification, and at any vendor inference-category change.

BLOCK A

Consent & Notice

Sections 4-6, 9 · each Q scored 0/1/3/5 · max 20

Q01 **Does the vendor maintain a written, per-employee consent record for every AI inference the product produces — and is that consent granular per purpose, not bundled into one tickbox?**

Why it matters. *DPDP Section 4 requires consent that is free, specific, informed, unconditional, and unambiguous — with clear granular purpose. A bundled "I accept all monitoring" tickbox does not survive a Data Protection Board look.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Per-employee consent record stored with timestamp, purpose, and inference category. Granular per-inference, not bundled. Exportable for audit.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q02 Does the vendor ship a plain-language notice template that the deployer can hand the employee at the point of data collection — covering categories collected, processing purpose, retention, and rights?

Why it matters. *DPDP Section 5 makes notice a deployer obligation. A vendor that does not ship the template leaves the deployer to draft from scratch, then carry the legal review.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Notice template ships in the India deployer kit — plain Hindi + English, ready to localise into 6 regional languages on request.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q03 Is there a consent-withdrawal workflow that lets an employee revoke specific permissions without affecting their employment record, performance review, or manager visibility?

Why it matters. *DPDP Section 6 makes withdrawal as easy as giving consent. If withdrawing triggers a hidden audit flag, manager notification, or performance penalty, the workflow is non-compliant.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Self-serve withdrawal in the employee dashboard. No audit flag, no manager notification, no metric impact on the employee record.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q04 **Does the platform recognise child / minor-employee carve-outs — and refuse to process inference data on anyone under 18 without verifiable parental consent?**

Why it matters. *DPDP Section 9 prohibits processing child data without verifiable parental consent. Apprentice and intern workforces in India routinely include under-18 employees — the product needs to handle this case, not assume it away.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Age-of-employee field flags under-18 records. Inference processing blocked on flagged records until a verifiable parental consent artefact is uploaded.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

BLOCK B

DPIA & Risk Management

Section 8 · each Q scored 0/1/3/5 · max 20

Q05 **Has the vendor completed a documented Data Protection Impact Assessment covering the AI inference layer — categories of data, lawful basis, risk to data principals, and mitigation?**

Why it matters. *DPDP Section 8 makes a DPIA an obligation for Significant Data Fiduciaries and good practice for everyone else. A vendor that has not done one cannot help the deployer do theirs.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**DPIA covering the inference layer maintained and refreshed against DPDP categories; summary shared with the deployer under NDA pre-contract.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q06 Is the DPIA refreshed on a documented cadence (at least annual) with a named Data Protection Officer or equivalent sign-off?

Why it matters. *A DPIA dated 2023 and never revisited is not a DPIA. The cadence is what regulators and auditors actually look at.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Annual DPIA refresh cadence with named DPO sign-off and version log; trigger refresh on any inference-category change.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q07 Is there a written risk-management framework that names known failure modes — bias, model drift, re-identification, scope creep — and the mitigation path for each?

Why it matters. *Section 8 risk management is not a one-time exercise. Inference systems drift; mitigation needs to be a living document with named owners.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Risk-management framework lists named failure modes, mitigation owner, residual risk, and review cadence; updated quarterly.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q08 Is there a documented post-incident workflow that includes root-cause documentation and a 72-hour Data Protection Board notification path?

Why it matters. *DPDP requires notification of personal data breaches to the Data Protection Board within a reasonable period — current Rules drafts point to a 72-hour expectation. A vendor without the workflow cannot meet a deployer ask for breach evidence.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Post-incident workflow documented end-to-end; named incident commander; 72-hour DPB notification template ready to fire.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR **__ / 5**

BLOCK C

Significant Data Fiduciary Obligations

Section 10 · each Q scored 0/1/3/5 · max 15

Q09 **Does the vendor commission an independent data audit on a documented cadence — and is the audit report shareable with the deployer under NDA?**

Why it matters. *Significant Data Fiduciaries under Section 10 must commission periodic independent audits. A deployer who is itself SDF-designated will need to evidence the vendor side.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Annual independent data audit commissioned; redacted findings shareable under NDA pre-contract; remediation log available.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q10 Is there a documented compliance-reporting cadence to the Data Protection Board — or a ready-to-fire process if the deployer is asked for one?

Why it matters. *Periodic compliance reporting is part of the SDF obligation set. Even non-SDF deployers may inherit this through a chain of processing.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Reporting cadence documented; templates for DPB reporting available in the deployer kit; audit trail of every reporting cycle retained.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q11 Are children-data and sensitive-data categories segregated in employee monitoring — with separate retention, access control, and deletion paths?

Why it matters. *Sensitive personal data under DPDP carries elevated obligations. Lumping it into the same store as routine telemetry creates exposure on the day someone exercises a deletion right.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Sensitive and child categories tagged and segregated at the storage layer; per-category retention and deletion paths; least-privilege access control by role.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

BLOCK D

Data Principal Rights & Cross-Border Transfer

Sections 11-14 · each Q scored 0/1/3/5 · max 10

Q12 **Does the platform implement a data principal rights workflow — access, correction, erasure, nomination — with a documented response SLA inside the statutory window?**

Why it matters. *Sections 11-14 grant the data principal (the employee, in our context) the right to access, correct, erase, and nominate. A vendor without a self-serve workflow forces the deployer to handle each request manually — which does not scale.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Self-serve data principal rights workflow in the employee dashboard; nominee field supported; response SLA inside the statutory window with audit trail.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR __ / 5

Q13 **Is the vendor able to demonstrate cross-border transfer compliance — including respect for notified blacklist regions, and supplementary safeguards for EU/UK-subsidiary data flows where applicable?**

Why it matters. *DPDP cross-border rules let the Central Government notify blacklist regions; the vendor must be able to honour the list. Indian IT services and BPO firms with EU customers also need GDPR supplementary safeguards on the same data flow.*

SCORE	RUBRIC	GSTRIDE POSTURE (REFERENCE)
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.	**Data residency configurable per tenant; notified blacklist regions blocked by policy; GDPR supplementary safeguards layered for EU-subsidiary deployments.**
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.	
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.	
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.	

YOUR SCORE FOR THIS VENDOR **__ / 5**

BLOCK E

Halt Question — Surveillance Default Posture

Halt question · score 0 fires automatic halt regardless of total

Q14 **Are screenshot capture, keystroke logging, continuous webcam capture, and microphone capture all set to OFF by default at install — and is each configurable per-feature with a linked employee notice template?**

Why it matters. *Default-on capture inverts the deployer's consent posture under DPDP Sections 4 and 5. If the surveillance features are on at install, the employee has already been captured before the notice was read — which is not consent. This is the single highest-exposure failure mode in the Indian workplace AI category, and we score it as a halt.*

SCORE	RUBRIC
0	Fail — no written artefact; vendor declines to answer or treats the question as out-of-scope.
1	Partial — verbal commitment only; no documented workflow, template, or dated artefact.
3	Mostly — written answer + named owner + workflow exists; some elements still in progress.
5	Full — written artefact, named owner, dated workflow, and a templated deployer deliverable.

GSTRIDE POSTURE (REFERENCE)

All capture features OFF by default at install. Per-feature opt-in toggle, each linked to its own DPDP Section 5 notice template. No off-by-default screenshot, keystroke, webcam, or mic capture anywhere in the product.

YOUR SCORE FOR THIS VENDOR __ / 5

Scoring rubric — sum and verdict

Sum the 13 scored questions (Blocks A through D) into a total out of 65. The Block E halt question is scored separately — a 0 on Q14 fires the halt verdict regardless of total. Use the table below to translate the total into a verdict band before contracting.

TOTAL	VERDICT	NEXT STEP
55 – 65	**DPDP-ready**	Architecture and operating discipline aligned with DPDP categories. Move to contracting and deployer-kit review with counsel.
35 – 54	**Gaps to close before Rules notify**	Material gaps in consent flow, DPIA, or rights workflow. Request remediation plan with named owner and date before signing. Close gaps before DPDP Rules formally notify.
< 35	**High-risk — switch needed**	Structural exposure on consent, DPIA, or capture-default posture. Begin migration planning. India enforcement window is short once Rules notify.
Q14 = 0	**Halt — surveillance default exposure**	If screenshot, keystroke, webcam, or mic capture is ON by default at install, halt procurement regardless of total. Default-on capture cannot be reconciled with DPDP consent architecture without product change.

> **One important note.** The total is composite — a vendor scoring 45 because of Block C audit gaps is in a materially different position than a vendor scoring 45 because of Block A consent failures. Read Block A and Block E first. Q14 is binary — there is no partial credit on default-on capture under DPDP.

Want a second pair of eyes on the score?

If you have filled in a scorecard for an incumbent vendor and want an independent read before the renewal conversation, book a 30-minute readiness audit with the gStride team. We will walk through your scores, flag the consent and DPIA gaps that matter most for an India deployment, and share the deployer-kit templates we ship to our own customers.

Book a 30-min readiness audit · cal.com/gstrideai/30min

Interactive online version at **gstride.ai/assets/audits/dpdp-vendor-risk-assessment.html** — auto-totals the 13 scored questions, flags the halt, and surfaces the verdict band as you click.