

DPDP Vendor Contract Compliance Checklist

24 checks for vendor agreements, DPAs and SaaS terms under the DPDP Act, 2023 and Rules, 2025

Prepared by ClauseAudit | As of October 2026 | Core duties apply from 13 May 2027

How to use this checklist

Work through each contract that lets a vendor hold or process personal data of your customers or staff. Tick a box only when the clause is actually in the signed document, including its schedules. Six checks come from the Act or Rules themselves and are marked LAW. The other eighteen are marked RECOMMENDED: the law does not require that exact clause, but the clause is how a data fiduciary meets a duty the law places on it, or how it protects itself. The basis line under each check gives the section or rule so you can read it yourself.

Who answers for the vendor: under section 8(1) of the Act the data fiduciary (usually the customer) is responsible for processing done on its behalf by a data processor (usually the vendor), irrespective of any agreement to the contrary. Under section 8(2) it may engage the processor only under a valid contract. From 13 May 2027 the Data Protection Board may impose penalties of up to Rs 250 crore for a significant failure to take reasonable security safeguards and up to Rs 200 crore for breach notice failures.

Required by the DPDP Act or Rules (6)

- ☐ **1. Processing runs under a valid contract; best practice is a written agreement or DPA covering the processing, with at least a security-safeguards provision (Rule 6(1)(f)).**
Red flag: No contract covers the vendor's processing, or the contract has no security-safeguards provision.
Basis: s.8(2) (valid contract); Rule 6(1)(f) (security-safeguards provision, wherever applicable). A written or signed DPA is recommended, not required.
- ☐ **2. Vendor must stop processing a named individual's data within a set time when the customer tells it consent was withdrawn.**
Red flag: No mechanism or timeline for the customer to make the vendor stop processing for specific individuals.
Basis: s.6(6) (fiduciary must, within a reasonable time, cause its processors to cease); a fixed contractual timeline is recommended
- ☐ **3. Vendor keeps access and processing logs (and the related personal data) for at least one year, unless another law requires longer, then erases them.**
Red flag: No logging duty, or logs kept for less than one year.
Basis: Rule 6(1)(e); Rule 8(3) with Illustration Case 2
- ☐ **4. Vendor must erase customer personal data on instruction and at termination, and certify erasure, subject to the one-year log minimum and any legal retention duty.**
Red flag: Vendor may retain data indefinitely or for its own purposes after termination.
Basis: s.8(7)(a), (b) (fiduciary must cause its processor to erase), subject to Rule 8(3); certification of erasure is recommended
- ☐ **5. If the customer is a large e-commerce, online gaming or social media platform in the Third Schedule, vendor supports three-year inactivity erasure and the 48-hour pre-erasure notice.**
Red flag: Vendor's retention settings cannot implement the customer's Third Schedule deletion cycle.
Basis: Rule 8(1), 8(2) and Third Schedule (only for the listed classes of fiduciary)
- ☐ **6. If children's data may be processed, vendor must not track, behaviourally monitor or target ads at children and must support verifiable parental consent.**
Red flag: Vendor may profile users or run targeted advertising without excluding children.
Basis: s.9(1) and 9(3); Rules 10, 11 and 12 with the Fourth Schedule (exemptions lift only s.9(1) and 9(3))

Recommended practice (18)

- ☐ **7. Identifies the customer as Data Fiduciary and the vendor as Data Processor, and limits the vendor to processing on the customer's behalf; processing on the customer's documented instructions is best practice (a GDPR Art. 28 concept), not a DPDP requirement.**
Red flag: No roles stated, or the vendor may decide its own purposes for the customer's personal data.
Basis: s.2(i), 2(k) (definitions only; no duty to label roles)
- ☐ **8. Gives the customer instruction, audit and information rights matching its continuing statutory responsibility.**
Red flag: Clause implies the customer is relieved of DPDP duties because the vendor processes the data, with no audit or information rights.
Basis: supports s.8(1)
- ☐ **9. Restricts vendor use of personal data to providing the contracted services within the purposes in the customer's notice.**
Red flag: Vendor may use customer personal data for its own product improvement, analytics, AI or model training, or marketing.
Basis: supports ss.5(1), 6(1)
- ☐ **10. If the vendor runs the notice or consent flow, it must present the customer's Rule 3 notice and keep notice and consent records available to the customer.**
Red flag: Vendor hosts consent capture but has no duty to keep or produce consent records.
Basis: supports Rule 3(a) to (c) and s.6(10)
- ☐ **11. Contains a security schedule covering encryption, masking or tokenisation, access control, logging and monitoring, backups and continuity, and technical and organisational measures.**
Red flag: Only a generic 'industry standard security' promise, with no specific measures (a best-practice risk, not non-compliance: Rule 6(1)(f) needs only an appropriate provision wherever applicable).
Basis: supports s.8(5) and Rule 6(1)(a) to (g); the contract needs only an appropriate provision under Rule 6(1)(f)
- ☐ **12. Vendor must notify the customer of any personal data breach within a fixed short period of becoming aware. This is a contractual recommendation: the Act and Rules set no vendor-to-customer deadline. The customer's own duties run from its awareness: first intimation to the Board and to individuals without delay, and the detailed report to the Board within 72 hours.**
Red flag: No fixed vendor notice period, or a period that would leave the customer unable to report to the Board without delay and within 72 hours of its own awareness.
Basis: supports s.8(6) and Rule 7(1), 7(2)(a), 7(2)(b); no processor deadline exists in law
- ☐ **13. Vendor breach notice must include nature, extent, timing and location, likely impact, mitigation, causes, findings on who caused it, and remedial steps, with updates.**
Red flag: Vendor need only say a breach occurred, or controls what information the customer receives.
Basis: supports Rule 7(1) and 7(2)
- ☐ **14. Vendor must cooperate with the customer's intimations to affected individuals and to the Data Protection Board.**
Red flag: Vendor may notify individuals or regulators itself without customer coordination, or refuses cooperation.
Basis: supports s.8(6) and Rule 7
- ☐ **15. Vendor must help the customer answer access, correction, completion, updating, erasure and nomination requests within set times.**
Red flag: No assistance duty, or assistance is refused or separately chargeable at the vendor's discretion.
Basis: supports ss.11 to 14

- ☐ **16. Vendor keeps a current list of sub-processors with the data shared, gives advance notice of changes, and flows down equivalent terms.**
 Red flag: Vendor may appoint sub-processors freely with no list or notice, so the customer cannot answer a s.11 access request.
 Basis: supports s.11(1)(b) and s.8(1)
- ☐ **17. Vendor resolves or supports complaints within a timeline that keeps the customer inside its grievance response period (not exceeding ninety days).**
 Red flag: No grievance support or timeline.
 Basis: supports s.8(10) and Rule 14(3)
- ☐ **18. Names a vendor privacy contact and the customer's DPO or contact person for data protection matters.**
 Red flag: No named data protection contact on either side.
 Basis: supports s.8(9) and Rule 9
- ☐ **19. States where data is stored and processed and requires notice before relocating it, plus compliance with any notified s.16 restriction or sectoral localisation rule.**
 Red flag: Vendor may transfer data to any country or sub-processor without notice.
 Basis: supports s.16 and Rule 15; following any notified s.16 restriction or other law restricting transfer is itself law, but none was located as of 26 Oct 2026
- ☐ **20. If the customer is or may be a Significant Data Fiduciary, vendor cooperates with annual DPIA and data audit and can keep specified data in India.**
 Red flag: No audit or DPIA cooperation, or no way to comply with a localisation direction.
 Basis: supports s.10(2) and Rule 13; any Rule 13(4) localisation direction would itself be law for an SDF
- ☐ **21. Where vendor output drives decisions about individuals, vendor supports accuracy checks and corrections.**
 Red flag: Vendor disclaims any responsibility for data accuracy in a decision-making service.
 Basis: supports s.8(3)
- ☐ **22. Data protection liability and indemnity are sized against the Schedule maximum penalties, which apply from 13 May 2027 and are imposed by the Data Protection Board only for a breach it finds significant, with the amount set using the s.33(2) factors (up to Rs 250 crore for security failures, up to Rs 200 crore for breach-notice failures; for breach of a voluntary undertaking, up to the penalty for the original breach). These are maximums, not fixed amounts.**
 Red flag: Data protection liability capped at a few months of fees, or data breaches excluded from indemnity.
 Basis: sized against s.33 and the Schedule (from 13 May 2027)
- ☐ **23. For an Indian vendor processing only non-residents' data under a foreign contract, the DPA reflects the s.17(1)(d) exemption but keeps security obligations.**
 Red flag: DPA drops security commitments on the basis that DPDP does not apply.
 Basis: reflects s.17(1)(d); s.8(1) and 8(5) still apply by law
- ☐ **24. Contract builds in DPDP obligations now, or a clause to adopt them automatically from the commencement date, since the term runs past 13 May 2027.**
 Red flag: Contract ignores DPDP because it is 'not yet in force' though its term extends beyond the commencement date.
 Basis: G.S.R. 843(E) paras (a) to (c)

Check a contract against all 24 points in minutes

Upload the vendor agreement, DPA or SaaS terms at clauseaudit.com/in/dpdp. Every clause is read against the DPDP Act and Rules, each finding is marked as required by law (with the section or rule) or recommended practice, and you get a suggested redline and a negotiation email. Choose the customer or the vendor side. Rs 999 per contract, paid once. The original document is not stored. It is an AI-assisted review and not legal advice; have an advocate check anything material before you sign.