Where can your data actually go?

A cross-border sheet for Indian companies — what the DPDP framework does, what it does not do, and what is actually constraining your data exports today.

> **What this is / is not.** This is general, illustrative and **non-exhaustive** information on cross-border personal-data transfer under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. It is **not legal advice**, **not a compliance certification or determination**, and does **not** create an advocate–client relationship. Not every item applies to every business, several of the provisions discussed are **not yet in force**, and the position on notified restrictions can change with a single gazette notification. A real assessment needs the facts of your own processing and your own sector. **Confirm commencement, notifications and sector rules for your own entity before acting.** Current as at 2 September 2026.
>
> *Prepared by Rushikesh Mahajan, Advocate.*

The short answer. Under the DPDP framework, personal data may go **anywhere** — until the Central Government names a country and shuts the door to it. On the public record, **no country or territory has been named**. And the provision that carries the power is **not yet in force**: Section 16 of the Act and Rule 15 of the Rules commence on **13 May 2027**.

Which means the rule constraining your data exports today is almost never the DPDP. This sheet is about finding the one that is.

1 · What Section 16(1) actually says — and what it does not contain

> *"The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified."*

Read what that sentence does *not* contain. There is no adequacy assessment. No standard contractual clauses. No binding corporate rules. No derogation architecture, no necessity test, no supplementary-measures analysis. There is a power in the Union Government to name a country and close it.

This is the **negative-list** model, and it is the mirror image of the European one. Under the GDPR a transfer out of the EEA is *prohibited unless* the exporter can point to a mechanism that permits it. Under Section 16 a transfer out of India is *permitted unless* the Government has pointed at the destination and forbidden it.

	GDPR, Chapter V	DPDP, Section 16
Default	Transfer prohibited	Transfer permitted
Model	Whitelist — adequacy decisions	Negative list — restriction by notification
Instruments	SCCs, BCRs, derogations, transfer-impact assessment	None. The Act creates no transfer instrument at all.
Who acts first	The exporter, to unlock the transfer	The Government, to block it
Status today	In force; adequacy list live	**Not in force until 13 May 2027; nothing notified**

2 · What Rule 15 is really about — and the drafting error it causes

It is worth reading the operative rule rather than the summaries of it. Rule 15 of the DPDP Rules, 2025, headed *"Transfer of personal data outside the territory of India"*, provides:

> *"Any personal data processed by a Data Fiduciary under the Act may be transferred outside the territory of India subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to **any foreign State, or to any person or entity under the control of or any agency of such a State**."*

The operative words are the ones in bold. The rule is not drafted around your cloud region or your Dublin analytics processor. It is drafted around the circumstance in which Indian personal data becomes available to a **foreign government** — its agencies, and entities under its control. That is a sovereignty and lawful-access concern, and it is a different anxiety from the commercial-processor anxiety that Chapter V of the GDPR addresses.

The mismatch produces a specific and repeated drafting error. Vendor questionnaires and data-processing addenda now recite "compliance with Rule 15 transfer requirements" as though Rule 15 had issued a set of clauses. It has not issued anything. It reserves a power to specify requirements by general or special order, and no such order is in the public domain.

3 · Section 16(2) — the sub-section that gets skipped

> *"Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data … outside India …"*

The DPDP framework sets a **floor, not a ceiling**, and it expressly steps aside for anything stricter. The clearest example is the Reserve Bank of India's directive of **6 April 2018** on storage of payment system data, issued under the Payment and Settlement Systems Act, 2007, which requires payment system operators to store the full end-to-end payment data — customer data, payment-sensitive data, payment creden-

tials, transaction data — within India. That directive is in force and it is enforced. Section 16(2) means the DPDP framework's permissiveness does nothing whatever to soften it. The same logic runs across the sectoral regulators.

4 · So what is actually binding your data exports — in order of how likely it is to bite

#	The constraint	Why it outranks what sits below it
1	**Your sectoral regulator**	Payments, banking, insurance, telecom and securities each carry their own data rules, and they outrank the DPDP framework by the express terms of Section 16(2). If you have a regulator, start here.
2	**Your counterparty's contract**	If a European or British customer's data-processing agreement obliges you to hold their data in a particular way, that binds you because you signed it — not because India requires it.
3	**The GDPR or UK GDPR, flowing the other way**	Where you receive European data, or offer into those markets, the European instrument reaches you directly. This is usually the hardest constraint an Indian technology business actually faces.
4	**Section 16 and Rule 15**	From **13 May 2027**, and then only to the extent something is notified under them. Today: nothing.

> *A readiness programme whose transfer workstream consists of mapping vendors against a list that does not exist, under a section that has not started, is not early. It is aimed at the wrong target.*

5 · The localisation power that does exist sits in Rule 12 — and it is aimed at SDFs

While Section 16 holds a restriction power that has not been used, **Rule 12** of the DPDP Rules, 2025 does something narrower and sharper. A **Significant Data Fiduciary** must undertake measures to ensure that personal data specified by the Central Government — on the recommendations of a committee constituted by it — is processed subject to the restriction that that personal data, **and the traffic data pertaining to its flow**, is not transferred outside India.

Two features are worth noting. The trigger is **SDF designation**, so it reaches only entities the Government has notified as significant. And the inclusion of **traffic data** is a meaningful extension: it is not only the payload that must stay, but the metadata of its movement. Like the rest of the substantive package, Rule 12 is not yet in force.

6 · The asymmetry, in one line

Europe built an institution for saying *yes*, and has said it to a list of jurisdictions it recognises as adequate. **India is not on that list.** India built a power for saying *no*, and has not yet used it once. The two architectures produce exactly opposite defaults — a European exporter must find a permission before data moves; an Indian exporter must find a prohibition before it stops.

An Indian company sitting between a European customer and an American processor is subject to both at the same time, pointing in opposite directions. That is the honest shape of cross-border work for an Indian technology business in 2026, and it is worth saying plainly: **the hard constraint is almost never**

Section 16. It is the European instrument reaching in, the sectoral regulator sitting above, and the contract already signed.

7 · The one-page test — "what would have to move?"

The cheapest insurance against a notification under Section 16 is not localisation. It is being able to answer, on one page, exactly which processing would have to move if a given country were named. Work through this for each destination country your data reaches.

- [ ] **Name the destination.** Not "the cloud" — the country. Region-level, for every service: primary storage, backups, disaster recovery, logs, analytics, support tooling, and any sub-processor of those.
- [ ] **Name what sits there.** Which categories of personal data, for which purpose, and whose — customers, employees, or someone else's data you hold as a processor.
- [ ] **Name the legal character of the recipient.** Is it your **processor** (acting on your behalf) or an **independent Data Fiduciary** (deciding its own purposes)? The answer changes what your contract has to carry, and getting it wrong is the most common early error.
- [ ] **Identify your sectoral overlay first.** If a regulator sits above you, write down which of its instruments touches this flow and whether it is stricter than the DPDP framework. If it is, it governs — Section 16(2).
- [ ] **Identify inbound European exposure.** Is any of this data received from an EEA or UK exporter, or is the service offered into those markets? If yes, the European mechanism applies in its own right and must be documented as such.
- [ ] **Answer the move question.** If this destination were notified as restricted, what breaks — and how long would relocation take? Record the answer in weeks, not adjectives.
- [ ] **Record what you would have to tell people.** Which notices, contracts and questionnaire answers would need revising if the flow moved.
- [ ] **Date the page and set a review.** The power in Section 16(1) is exercisable by notification, with no consultation period written into the section and no transition. A company whose architecture assumes a particular jurisdiction is fine has taken a position on future government policy, and should know that it has.

8 · What an Indian data-processing schedule should carry instead

A clause reciting "the parties shall execute Standard Contractual Clauses as required under the DPDP Act" is describing an instrument that does not exist in Indian law. Stop writing transfer mechanisms into Indian contracts that have none to write. What the schedule should actually carry:

- [ ] The **Section 8(2)** processor obligation — a processor may be engaged only under a valid contract.
- [ ] **Security expectations**, stated concretely enough to be audited rather than recited.
- [ ] The **breach-notification chain**, with the vendor's time to tell you set shorter than your own time to tell the Board.
- [ ] **Deletion on termination**, and the ability to make a sub-processor delete too.

- [ ] A **sub-processor** gate — who they may onboard, and how you find out.
- [ ] Where the counterparty has European exposure, **the European mechanism in its own right, correctly labelled** — not folded into an Indian clause that cannot carry it.

9 · The dates that matter

Date	What it is
6 April 2018	RBI directive on storage of payment system data — **in force now**, and preserved over the DPDP framework by Section 16(2)
13 November 2025	Digital Personal Data Protection Rules, 2025 notified
13 November 2026	Consent-Manager package commences (Rule 4 / s.6(9)) — the only substantive obligations that start before 2027
13 May 2027	**Section 16 + Rule 15 (cross-border) commence**, together with notice, security safeguards, breach reporting, retention and children's data

> *Dates are stated absolutely and deliberately: this sheet is meant to still read correctly whenever you open it. Nothing above is a countdown.*

10 · The pattern to carry out of this sheet

India did not translate the GDPR. It borrowed the vocabulary — *data principal* for data subject, *data fiduciary* for controller, a consent architecture that looks familiar at a distance — and then made materially different structural choices underneath. The transfer regime is a negative list, not an adequacy regime. Section 7's legitimate uses are a **closed list of enumerated categories with no balancing test**, and are not the GDPR's legitimate-interests ground wearing an Indian name.

Every place where the vocabulary matches and the structure does not is a place where a GDPR-trained instinct produces a confident, well-drafted, wrong answer. Cross-border is simply the clearest example.

Prepared by Rushikesh Mahajan, Advocate. Statutory text, rule text and commencement dates verified against public sources; the status of notifications under Section 16 is stated as it appears on the public record as at 2 September 2026 and can change without notice. Longer treatments of these questions appear fortnightly at The India Data & AI Governance Desk — buttondown.com/the_desk/archive.