

Delegation and accountability for agents under the DPDP Act

Version 0.1 · Published · 12 October 2026

ABSTRACT

India's Digital Personal Data Protection Act, 2023 assigns duties by role, to data fiduciaries, data processors, data principals and consent managers. It does not mention an AI agent acting for a person. This paper maps those roles onto an agent's delegation chain in three common set-ups, proposes a delegation reference that travels with personal data an agent forwards (labelled as our reading and a proposal, not a legal requirement), raises the position of consent managers as an open question, and lists the gaps we found in the Act and the Rules. It is a basis for discussion with counsel and regulators.

READ THIS FIRST

This is a position, not a specification, and not legal advice. It is a basis for discussion with counsel and regulators. The set-ups and the patient's family below are invented. Check anything that matters with counsel.

Start with a made-up evening in Coimbatore.

A man in his forties uses a personal assistant agent to look after his mother's health paperwork. She lives alone and has diabetes. One evening the agent asks her diagnostic lab for her latest blood test report. The lab sends it. The agent then forwards the report to a summarising service, so it can give him three plain sentences about what changed. Later it books a follow-up appointment with her doctor's clinic and attaches a line from the report.

Count the parties. The mother, her son, the assistant and whoever runs it, the lab, the summarising service (which may run on someone else's cloud) and the clinic. Personal data about one woman has passed through at least four organisations in an hour, on the say-so of a piece of software.

Suppose she later asks the lab, in writing, where her report went. Or suppose the summarising service has a breach. Who answers, to whom, and how would anyone find out which path the report took?

India's data protection law has a lot to say about roles. It says nothing about the assistant. This paper is our attempt to map one onto the other, to propose one practical habit that would help, and to be honest about where we couldn't tell.

What we read, and how

We read the primary texts. The Digital Personal Data Protection Act, 2023 is in the Gazette Extraordinary of 11 August 2023 (<https://egazette.gov.in/WriteReadData/2023/248045.pdf>). The Digital Personal Data Protection Rules, 2025 are in the Gazette notification G.S.R. 846(E) of 13 November 2025 (<https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>), which we read as published by the Ministry of Electronics and Information Technology. The dates on which parts of the Act start are in a separate notification, G.S.R. 843(E), of the same day (<https://egazette.gov.in/WriteReadData/2025/267647.pdf>). We read all three on 12 October 2026. The

official files opened for us, so we didn't need to rely on a secondary reproduction for any provision we quote. We also found a copy of the Act on the PRS Legislative Research site that turned out to be byte for byte the same file as the Gazette. Where we quote a section or a rule, we have checked the wording against the official file.

A few honest limits. We haven't read any lawyers' commentary, court decision or guidance from the Data Protection Board, and we don't know whether such guidance exists. We haven't checked whether the government has issued any of the orders the Act and the Rules say it may. And we've read the English text only.

When any of this starts to apply

The dates matter, because most of the duties discussed below aren't running yet.

The commencement notification splits the Act into three. Section 2, which holds the definitions, the sections that set up the Data Protection Board, and a few others came into force on publication. Section 6(9), which says every Consent Manager must be registered with the Board, and section 27(1)(d), come into force a year after publication. Most of the rest, including sections 3 to 5, 6(1) to 6(8) and 6(10), sections 7 to 17 and the Board's enforcement powers, come into force eighteen months after publication.

The notification is dated 13 November 2025. Counting from that date, the one-year provisions start on 13 November 2026 and the eighteen-month provisions on 13 May 2027. The government's [press release](https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014>) says the Rules were notified on 14 November, so the dates may fall a day later. The Rules follow the same pattern: Rule 4 on consent managers comes a year after publication, and Rules 3 and 5 to 16 eighteen months after.

A correction of our own: some earlier articles said sections 3 to 17 all start on 13 May 2027. Section 6(9) starts a year after publication, so that was slightly off for one subsection. We've corrected those articles.

In practice this means that, on our reading, the duties to give notice, take consent, keep data safe or erase it aren't in force today. Anyone building now is building for a date that is coming.

Which words in the Act do the work

The Act is written by role. These are the definitions we lean on, all from section 2.

A **Data Principal** is "the individual to whom the personal data relates". Where that individual is a child, the term includes the parents or lawful guardian, and where she is a person with disability, it includes her lawful guardian.

A **Data Fiduciary** is "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data".

A **Data Processor** is "any person who processes personal data on behalf of a Data Fiduciary".

A **Consent Manager** is "a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform".

"Person" includes an individual, a Hindu undivided family, a company, a firm, an association of persons, the State, and "every artificial juristic person, not falling within any of the preceding sub-clauses". Nothing in the list names software. "Processing" includes collection, storage, use and "sharing, disclosure by transmission, dissemination or otherwise making available", so an agent forwarding a report is processing.

Two things follow. First, an agent isn't a role in the Act. As far as we can tell, neither the Act nor the Rules uses the word "agent" in the sense this paper does, or mentions artificial intelligence. Second, an agent is not a person in the Act's sense on any reading we can see, so a person has to be answerable for it. That is the owner, in our first paper. The question is which of the Act's roles that owner, the agent and the others in the chain fall into. It depends on who decides why and how the data is used.

Three set-ups, and the role each one gets

Using the words above, we think an agent's situation falls into one of three set-ups, and that the delegation chain is what tells you which one you're in. This is our reading and we'd like it tested.

Set-up	Who decides why and how the data is used	Our reading of the roles
The agent is the person's own tool	The person, for her own affairs	The Act doesn't apply to personal data "processed by an individual for any personal or domestic purpose" (section 3(c)(i)). The moment the agent sends data to an organisation, that organisation is within the Act.
The agent is a service run by a company for the person	The company, for the service it offers, and the person, by choosing it	The company looks like a Data Fiduciary toward the person, with notice and consent duties. The office receiving the data from it is a Data Fiduciary too, and the company is another one.
The agent is engaged by the office itself	The office	The agent's operator looks like the office's Data Processor, which section 8(2) allows "only under a valid contract".

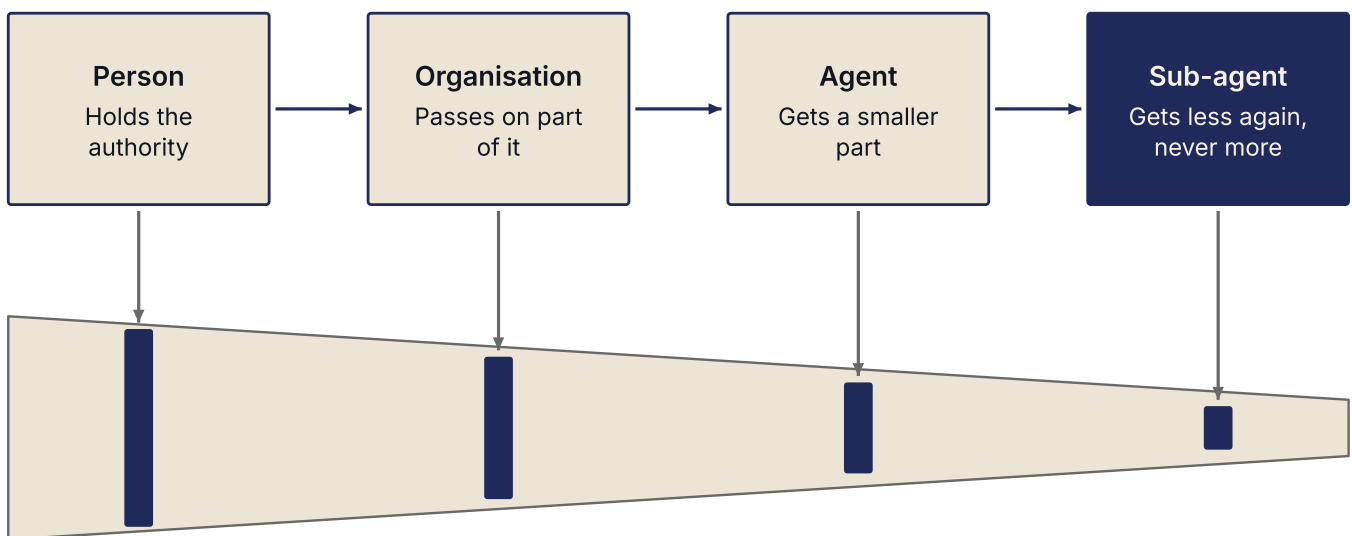
The first set-up is the son's own tool in our Coimbatore evening, if he runs it himself. Even there it's not clear-cut, because the data is about his mother, and whether looking after a parent's paperwork is "personal or domestic" is a question for counsel. The second is the same assistant, if a company runs it. The third is a lab that hires a scheduling agent from a vendor to handle its own bookings.

Why does the table matter? Because the duties differ. A Data Fiduciary must give notice and obtain consent (sections 5 and 6), and under section 8(1) is responsible for processing done on its behalf "irrespective of any agreement to the contrary". It must ensure "completeness, accuracy and consistency" of data likely to be disclosed to another Data Fiduciary (section 8(3)(b)). A Data Processor, by contrast, acts on the fiduciary's instructions, and the fiduciary has to cause it to erase data (section 8(7)(b)) and to stop processing when consent is withdrawn (section 6(6)).

The office at the front door usually can't tell which set-up it's in. It sees a request. A delegation chain that names who the agent works for, and who engaged it, is what would let it tell.

Authority chain and data chain are not the same chain

There's a distinction that took us a while to see. A delegation chain, as we use the term, is about authority: the person gave some to an organisation, which gave part of it to an agent, which may have handed part to a helper. Each link can pass on only part of what it received.



What each may do

Figure 1. Authority passes down from a person to an agent, and gets smaller at each step.

► Read this diagram as text

1. It starts with a person, who holds the authority to act.
2. The person passes part of that authority to an organisation.
3. The organisation passes a smaller part to an agent.
4. The agent can pass a smaller part again to a sub-agent.
5. At every step the band gets narrower, because nobody can hand on more than they were given.

The Act is concerned with a different chain, the data chain: who collected the personal data, who it was shared with, who processed it on whose behalf. The two often run side by side. They aren't the same. A helper agent may hold a sliver of authority and never touch the data. A cloud service may hold all the data and hold no authority from anyone.

Accountability under the Act runs along the data chain. The data fiduciary is responsible for processing "by it or on its behalf by a Data Processor". So for a regulator, the interesting question is who touched the data and on whose behalf. For the person, it's who was allowed to act for her. A good record answers both, and ties them together.

Consent that arrives through an agent

Section 6(1) says consent must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action", and "limited to such personal data as is necessary for such specified purpose". Section 5 says a request for consent must be accompanied or preceded by a notice "given by the Data Fiduciary to the Data Principal". Section 2(za) defines the "specified purpose" as the purpose in that notice.

Now put an agent in the middle.

If the agent clicks accept, who has given consent? If the notice is shown to the agent, was it "given" to the Data Principal? Does a standing instruction such as "handle my mother's health bookings" count as a "clear affirmative action" for each purpose that comes up later? The wording suggests consent is meant to be specific to a purpose. A blanket permission of the "allow always" kind sits uneasily beside that, and we've said why we don't like it in [our piece on Muse](https://saakshya.org/articles/muse-can-act-for-you) (saakshya.org/articles/muse-can-act-for-you). We don't know whether a regulator would agree that a task-scoped delegation can carry a person's consent for the task. We'd say it should be able to, if the person saw the notice and the delegation names the purpose. The Act doesn't say.

Section 7(a) is another route. A Data Fiduciary may process data for "the specified purpose for which the Data Principal has voluntarily provided her personal data", unless she has indicated she doesn't consent. Does a person "voluntarily provide" her data when her agent sends it? We read the broker illustration in the Act as an everyday message from a person to a broker. An agent's message is the same kind of act at one remove, and we'd like counsel's view on whether it counts.

One more provision matters. Where consent is the basis of processing and a question arises in a proceeding, section 6(10) says "the Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal". The burden is on the fiduciary. So an office that relies on consent conveyed through an agent has to be able to prove it, and "the agent told us" is a weak proof. Our reading is that the office needs something it

can show: who the agent was, who stood behind it, what the person was told and what she agreed to. That is where a delegation reference could help, and it's the main reason we're writing this paper.

A delegation reference that travels with the data

This section is a proposal and our reading. Nothing in the Act or the Rules requires it.

The idea is simple. When an agent forwards personal data, a short delegation reference goes along with it. The reference points to the authority under which the agent is acting. A later reader should be able to follow it to answer four questions: who authorised this agent to act, which agent forwarded the data, for what purpose, and within what limits. We aren't going to say what the reference is made of or how it is written. That belongs in a specification, and the idea works at the level of function.

Here is why we think it fits the law's shape, provision by provision.

Section 11(1)(b) gives a person the right to obtain "the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared". An office that can't tell who an agent forwarded data to can't answer that.

Section 8(7)(b) requires a fiduciary to "cause its Data Processor to erase" data it made available, and section 6(6) requires it to "cease and cause its Data Processors to cease" processing when consent is withdrawn. You can't cause a party to do something if you can't find it.

Rule 7 is about breach. The Board must be told, within seventy-two hours, "any findings regarding the person who caused the breach", and each affected person must be given a description of the breach, "including its nature, extent and the timing of its occurrence". In the Coimbatore evening, a breach at the summarising service is very hard to describe to the mother if the lab never knew that service existed.

Rule 6(1)(c) lists, as a minimum security safeguard, "visibility on the accessing of such personal data, through appropriate logs, monitoring and review". Rule 8(3) requires personal data and logs of processing to be kept for at least a year, for the purposes in the Seventh Schedule. A reference that appears in those logs makes them readable.

And section 6(10), above, puts the burden of proving consent on the fiduciary.

The reference has limits, and we want them stated. It doesn't prove that the person consented, only that someone says the agent was authorised. It is no substitute for the valid contract that section 8(2) requires with a processor. It breaks if a downstream system drops it, and we have no way to make a downstream system keep it. It adds a field to every message. And a reference that carried personal data itself would defeat the purpose, so it should point at the authority and carry nothing about the person that the next reader doesn't need.

We made a similar argument from the phone's side in [Local processing is not local authority](https://saakshya.org/articles/local-processing-is-not-local-authority) (saakshya.org/articles/local-processing-is-not-local-authority). The reading of the Act there is the same as this one.

Consent managers and delegation: an open question

The Act's one named intermediary is the Consent Manager. Section 6(7) says a Data Principal "may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager". Section 6(8) says the Consent Manager "shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed".

That sounds a lot like what an agent does, and it's tempting to say an agent is a Consent Manager. We don't think it is, for a plain reason: the definition requires registration with the Board, and the Rules set conditions.

Rule 4 and its First Schedule say what those are. The applicant must be a company incorporated in India, with sufficient technical, operational and financial capacity, and independently certified as consistent with the Board's standards. Once registered, the Consent Manager must act "in a fiduciary capacity in relation to the Data Principal". It must make sure that the way personal data is made available or shared is such that "the contents thereof are not readable by it". It must keep a record of consents given, denied or withdrawn, of notices, and of "sharing of her personal data with a transferee Data Fiduciary", must keep that record for at least seven years, and must not subcontract its obligations. It must also avoid conflicts of interest with Data Fiduciaries.

Read those together and you get a picture: a neutral conduit that doesn't read the data and doesn't work for the organisations asking for it. An agent that reads the data to do a task, and may be run by a company with commercial ties to the organisations it deals with, doesn't look

like that. We read the two roles as meant to stay apart.

Rule 4 isn't in force yet. On our reading, no Consent Manager can be registered before it starts, and we don't know of any that has been.

That leaves questions we can't answer.

Can a person use an agent to carry out her consent decisions without any Consent Manager? The Act names one route, and it doesn't say it's the only one. It doesn't prohibit a person from asking a helper to act. It also doesn't recognise one, outside the cases of guardians (section 2(j)) and the nominee for death or incapacity (section 14).

Would a Consent Manager want to record a delegation? The records Rule 4 requires cover consents, notices and sharing. A delegation to an agent sits close to all three. Whether a Consent Manager should know which agents a person has authorised, and whether that sits comfortably with its duty not to read the contents, we don't know.

Could an agent platform register as a Consent Manager and still do agent work? The conflict and readability duties suggest not, at least for the same data. That's a question for the Board and for counsel.

Gaps we found

We kept a list while reading. Each item is a place where we couldn't find an answer in the text.

No representative other than a guardian or a nominee. The Act lets a guardian act for a child or a person with disability, and lets a person nominate someone for the event of death or incapacity. Rule 14(4) says she may "nominate one or more individuals". Nothing covers an ordinary adult who asks a helper, human or software, to act for her while she's perfectly capable.

Who gets the notice. Section 5 and Rule 3 describe notice from the fiduciary to the Data Principal. If the person only ever meets the agent, the notice may only ever meet the agent.

Children and agents. Rule 10 requires a fiduciary to observe due diligence in checking that "the individual identifying herself as the parent is an adult who is identifiable". It describes ways to check. It doesn't say what happens when a software agent says it acts for the parent. We don't know how a fiduciary would satisfy that rule through an agent.

Logs and delegation records. Rule 8(3) requires "logs of the processing" for a year. It doesn't say whether the record of who authorised an agent counts as part of those logs. We'd keep it with them.

Breach and the unnamed helper. Rule 7(2) asks for findings about "the person who caused the breach". A helper agent nobody recorded is a person who can't be named.

Data sent abroad. Section 16 and Rule 15 allow transfers outside India subject to requirements the government may set for a foreign State or its entities. We haven't looked for any order made under Rule 15 and can't say whether one exists. We do know that an agent on a foreign cloud puts the fiduciary's section 8(1) responsibility in play, whichever country the processing happens in.

What "processor" means for an agent the office didn't hire. Section 8(2) speaks of a processor engaged by the fiduciary under a contract. In the second set-up above, the office didn't engage the agent. The person did, or a company did. So the agent is probably not the office's processor, and the usual contractual comfort isn't there. We don't know what the Act expects in its place.

Questions we have not answered

We'd rather put these on the table than tidy them away.

Open questions about roles and consent

Is an individual's own agent doing "personal or domestic" processing under section 3(c)(i) when it handles a parent's paperwork? We're not sure.

Does a delegation that names a purpose count as a "clear affirmative action" for that purpose under section 6(1)? Does a standing instruction? Where is the line?

When her agent sends a person's data to an organisation, has she "voluntarily provided" it for section 7(a)?

Who is the Data Fiduciary when several parties each decide a little of why and how? The definition allows "alone or in conjunction with other persons", and we don't know how a regulator would carve up an agent chain.

What we don't know about timing, practice and the Board

We don't know how the Data Protection Board will treat agent activity. We haven't seen any guidance and we don't know whether any is planned.

We don't know whether a regulator would accept a delegation reference as part of the evidence a fiduciary needs under section 6(10), or whether it would want more.

We don't know how long delegation records should be kept. Rule 8(3) sets a floor of one year for logs of processing, and a Consent Manager's records must be kept for seven. Which, if either, applies to a delegation record is unclear.

We don't know whether our three set-ups are the right way to cut the problem. Real arrangements will be messier.

And we haven't considered other laws that sit beside the Act, in banking, health or tax. Section 38 says the Act is "in addition to and not in derogation of any other law", with the Act prevailing in a conflict. That makes the sector rules matter, and we haven't read them.

How to respond

Write to contact@saakshya.org. If you're a lawyer, the most useful thing you can do is tell us which of our readings you'd change and why. If you work for a regulator or the Board, we'd like to know whether any of these questions is already settled, and where. If you build or run agents, tell us which of the three set-ups you're in.

Saakshya is a non-profit we're setting up, and it isn't incorporated. It is independent of NPCI, UIDAI, MeitY, RBI, W3C and every company named in these papers, and none of them has endorsed this paper. This is version 0.1, dated 12 October 2026.

How to cite this paper

PLAIN TEXT

Saakshya (2026). Delegation and accountability for agents under the DPDP Act (Version 0.1).
Saakshya Position Paper 3. <https://saakshya.org/papers/delegation-and-accountability-under-the-dpdp-act>

BIBTEX

```
@techreport{saakshya_delegation_and_accountability_under_the_dpdp_act_v0_1,  
  title      = {Delegation and accountability for agents under the DPDP  
Act},  
  author     = {Saakshya},  
  institution = {Saakshya},  
  year       = {2026},  
  number     = {Position Paper 3},  
  type       = {Position paper},  
  version    = {0.1},  
  url        = {https://saakshya.org/papers/delegation-and-accountability-  
under-the-dpdp-act},  
}
```

Version history

Version 0.1 · 12 October 2026

First version.
