Association of
Independent Data Auditors
of India
www.aidai.org.in
A Division of Foundation of Data Protection Professionals in India

FDPPI – AIDAI

Understanding the Code of Professional Ethics

Frequently Asked Questions for Independent Data Auditors

Companion to Code version V15092026

This FAQ explains the FDPPI-AIDAI Code of Professional Ethics for Independent Data Auditors in the form it takes after the September 2026 revision, which added the clauses needed for multi-unit audits conducted under DGPSI-SOP600.

It is an explanatory note. Where this FAQ and the Code differ, the Code governs, and where the Code and DGPSI-SOP600 differ on a matter of audit procedure, the SOP governs. Clause references in the margin point to the Code; paragraph references in square brackets point to DGPSI-SOP600.

In this FAQ

A. The Code and its Status

Q1. Who is bound by this Code?

Every Data Auditor empanelled with AIDAI, in every engagement in which the auditor acts. It binds an auditor acting alone on a single-entity audit, an auditor acting as Lead Enterprise Data Auditor for a multi-unit entity, and an auditor acting as Component Data Auditor for one branch of that entity. The obligations attach to each auditor individually and are not shared out or diluted because the work has been divided.

Code reference: Objectives; A.5

Q2. Is the Code legally enforceable? AIDAI is not a statutory body.

Not as law, and the Code says so plainly. AIDAI is a self-regulatory body constituted by FDPPI, a Section 8 company. It derives no authority from an Act of Parliament, cannot compel testimony or the production of documents, cannot impose a fine or award damages, and cannot suspend anyone's right to practise as a data protection professional.

What makes the Code binding is contract. Every auditor gives an undertaking at empanelment, and on each renewal, to comply with the Code and with the SOPs AIDAI issues. Continued empanelment is conditional on that undertaking being honoured. So the enforcement question is not "can AIDAI punish me" but "do I wish to remain on the panel".

Code reference: Enforcement 2, 3 [SOP600 paras 30, 31, 35]

Q3. So what can AIDAI actually do if I breach it?

Four things, and nothing beyond them: close the matter with no action; record a written advisory or warning on your empanelment file; suspend your empanelment for a specified period; or cancel it. Suspension is the primary sanction and cancellation is reserved for appropriate cases. There is no monetary penalty and no finding that binds a court.

Code reference: Enforcement 3 [SOP600 paras 35, 36(d)]

Q4. Why was the Code revised in September 2026?

Because DGPSI-SOP600 introduced a way of working the earlier Code did not contemplate. Once an enterprise audit is split between a Lead Enterprise Data Auditor and several Component Data Auditors, questions arise that a single-auditor code has no answer to: how independent must the auditor of a branch be from that branch's own manager, what candour do two auditors owe each other when they have no contract between them, and what happens when one of them leans on the other to soften a finding. The revision adds those rules and leaves the five Core Ethical Principles untouched.

Code reference: Schedule of Changes

Q5. Does the Code change my obligations under the DPDPA?

No. The Code is a professional standard, not a source of statutory duty. Your obligations under the DPDPA 2023 and the ITA 2000 stand on their own, and clause A.2 requires you to observe them. In several places the Code asks more of you than the law does — the independence standard in B.4 is the clearest instance — but it never asks less.

Code reference: A.2; B.4

B. Independence and Conflicts of Interest

Q6. I am not an employee of the company I am auditing. Is that not enough independence?

No. “Not an employee” is the minimum the law may be read to require. It is a floor, not the professional standard.

What the Code expects is the fuller independence of clauses B.1 to B.3: no relationship that impairs, or would be presumed to impair, an unbiased assessment; active identification of self-interest and familiarity threats; and disclosure of facts that, if withheld, would distort the reported compliance position. An auditor who describes the statutory minimum as the professional standard is himself in breach of B.4.

> **Example.** You hold a modest shareholding in a listed bank and are offered the enterprise data audit. You are not an employee, so the statutory test is satisfied. B.2 is not: this is a self-interest threat and must be addressed, by disposing of the holding or by declining the engagement.

Code reference: B.1 to B.4

Q7. I audited a college's head office last year. Can I audit one of its departments this year?

Ordinarily yes — that is continuity, not conflict. Watch the familiarity threat under B.2 if the association becomes long, and watch B.6 if what you did earlier was scoping rather than auditing.

Code reference: B.2, B.6

Q8. I helped the client prepare its Implementation Charter. Can I now audit against it?

Not without AIDAI's written concurrence recorded in advance. The Implementation Charter records the deviations management approved after the gap assessment. If the same auditor both validates those deviations and then audits against them, management's choices have effectively set the scope of the audit that is supposed to test them.

The cleaner course, and the one the framework prefers, is that one Empanelled Data Auditor does the scoping and charter validation, and a different one conducts the audit.

Example. A hospital group's charter records that three of fifty DGPSI specifications will not be implemented at unit level on cost grounds. If you validated that charter, you cannot then issue the audit opinion that treats those three as properly out of scope.

Code reference: B.6

Q9. The client has offered a fee linked to the Data Trust Score. May I accept?

No. A fee contingent on the opinion expressed, on the Data Trust Score awarded, or on the report being free of qualifications is prohibited outright. So is any benefit from the entity or from one of its Units beyond the agreed professional fee and reimbursement of expenses. The objection is not that you would necessarily be swayed; it is that the arrangement makes your opinion purchasable on its face.

Code reference: B.7

Q10. I have been appointed Component Data Auditor for a branch. The branch manager is a former colleague and a personal friend. Does it matter, since the head office appointed me?

It matters. B.5 requires the Component Data Auditor to be independent of the management of the Unit audited, not merely of the entity at the apex. Central appointment and central payment do not cure a local relationship. The person whose controls you are testing, whose evidence you are accepting and whose explanations you are weighing is the branch manager. If the relationship would be presumed to impair an unbiased assessment, decline that Unit and ask to be assigned another.

Code reference: B.5

Q11. As Lead Enterprise Data Auditor, must I accept the component auditors the client nominates?

No, and you should not accept one where the circumstances of the nomination would compromise that auditor's independence. You must also record the basis on which each Component Data Auditor was accepted, so that the decision can be reviewed later.

Example. A bank proposes that each zonal office appoint its own auditor, and one zone nominates a firm that has provided data-protection consultancy to that zone for three years. The nomination compromises independence at the Unit level; say so in writing and ask for an alternative.

Code reference: B.8 [SOP600 paras 13, 32]

C. Acting as Lead Enterprise Data Auditor

Q12. What is the difference between a Lead Enterprise Data Auditor and a Lead Data Auditor?

A Lead Enterprise Data Auditor consolidates work done by auditors outside his own firm. He issues the Data Audit Report for the entity as a whole, incorporating the results of Unit audits performed by other Empanelled Data Auditors who are independent of him.

A Lead Data Auditor is the apt description where a group of data auditors of the same firm undertake an audit led by one senior person. The team is his own; the responsibility within the firm is his.

The ethical questions in Section E arise mainly in the first situation, because the two auditors are independent professionals with no contract between them.

Code reference: Terminology [SOP600 para 5]

Q13. How much of the entity must I audit myself before I can lead?

The Code does not fix a percentage. It requires you to satisfy yourself, before accepting, that your own participation will be sufficient to support the consolidated opinion, judged on four things: the materiality of the portion of the footprint you will personally audit; your knowledge of the business, data flows and systems of the Units; the risk of material non-compliance at Units audited by others; and your ability to perform the additional procedures the SOP requires.

Accepting the lead role without that capacity is a breach of the Code, whatever the commercial attraction of the engagement.

> **Example.** A bank with 900 branches offers you the enterprise audit on terms that allow you to visit four branches and read the reports for the rest. If you cannot properly review the component work in the time and fee available, the honest answer is to renegotiate the engagement or decline it.

Code reference: D.4 [SOP600 para 11]

Q14. If I rely on a Component Data Auditor's report and it turns out to be wrong, am I responsible?

You remain answerable for the consolidated Data Audit Report. Reliance is not abdication. You would not ordinarily be held responsible for the work entrusted to a component auditor, but that protection falls away in circumstances that should have aroused your suspicion — an unexplained departure from DGPSI methodology, or evidence inconsistent with the conclusions stated.

What you must never do is represent to the entity, to AIDAI or to anyone else that reliance on a fellow auditor displaced your responsibility.

Code reference: E.1 [SOP600 paras 14, 28]

Q15. What must I tell the component auditors at the start?

The use to be made of their work and report; the DGPSI control areas needing special consideration; the procedures for identifying personal data flows between Units; and the timetable. A component auditor who does not know that his report will be consolidated into an enterprise opinion cannot calibrate his work to that use. Withholding the context is treated as a failure of candour, not merely a planning lapse.

Code reference: E.3 [SOP600 para 14(a)]

Q16. Can I communicate with component auditors informally — phone calls and messages?

You may talk to them as often as you like, but the co-ordination itself must run through the standard communication procedure AIDAI prescribes, so that it can be evidenced afterwards. An engagement in which the only record of co-ordination is a set of phone calls cannot be reviewed, and clause E.5 treats substituting informal contact for the prescribed procedure as a breach.

Code reference: E.5 [SOP600 para 21; Annexure A]

Q17. A component auditor has sent me a clean report but I have doubts about the depth of the work. What should I do?

Apply the procedures the SOP gives you: discuss the audit procedures applied, review a written summary or completed questionnaire, visit the auditor if necessary, and perform supplemental tests of the Unit's records where you think them needed.

If you conclude the work cannot be used and you cannot perform sufficient additional procedures yourself, you must qualify the consolidated report, express the opinion or Data Trust Score subject to a limitation of scope, or decline to express an opinion for the entity as a whole — disclosing the reasons. What you may not do is resolve the difficulty by silence.

Code reference: E.11 [SOP600 paras 15, 18, 25]

Q18. One of the Units is audited by someone who is not empanelled with AIDAI. Is that permitted?

It can happen — most obviously where a Unit sits outside India and local law requires someone else. But you take the risk entirely. You must independently satisfy yourself of that person's competence and independence and document having done so.

Critically, you must not suggest, expressly or by implication, that AIDAI's empanelment-based assurance extends to that person's work. It does not.

Code reference: E.9 [SOP600 paras 13, 19, 32]

Q19. May I aggregate Unit results that were audited to a different standard?

No. Consistency of scope, procedures, evidence and reporting is the condition on which aggregation is defensible at all. Aggregating audits performed to different standards produces a number that looks like enterprise assurance but is not, and clause E.10 treats that as a misrepresentation of the assurance obtained.

> **Example.** Eleven branches were audited against DGPSI-Banks; two were audited against a general data-protection checklist an internal team preferred. Those two cannot be folded into the consolidated score without qualification.

Code reference: E.10

Q20. Must the consolidated report name each component auditor?

No. The report should indicate, at a summary level, the number and nature of Units audited by component auditors as distinct from those you audited directly, and state the division of responsibility — for example the number of branches audited by others and the proportion of the entity's footprint they represent. The names and empanelment numbers stay in your working papers and are produced to AIDAI on request.

Code reference: E.8 [SOP600 paras 27, 29]

D. Acting as Component Data Auditor

Q21. The Lead Enterprise Data Auditor is pressing me to withdraw a finding. What do I do?

Do not yield. Clause E.6 cuts both ways: the lead auditor must not press you to withdraw, dilute or reclassify a finding, and you must not give way if he does.

Record the disagreement in your working papers; he must record it in his. If it bears on the consolidated opinion, it goes to AIDAI. A difference of professional judgment between two competent auditors is not a disciplinary matter — concealing it is.

Code reference: E.6

Q22. I have been offered a component appointment with a scope that excludes the Unit's largest processing activity. May I take it?

Not on those terms silently. If the restriction is such that your report would be liable to mislead the Lead Enterprise Data Auditor, you must not accept it, and any restriction must be disclosed in writing before you accept. A narrow scope openly declared is a legitimate engagement; a narrow scope concealed behind a clean report is not.

Code reference: E.2

Q23. I have found something serious at my Unit. Do I wait for my report, or raise it now?

Raise it now. Significant findings requiring attention at the entity level go promptly to the Lead Enterprise Data Auditor. The consolidated audit may need to change course, and a finding delivered at the end of the timetable may arrive too late to matter. Softening or deferring a finding for the convenience of the Unit or the timetable is a breach.

> **Example.** You discover mid-audit that a branch has been sharing customer contact lists with a local insurance agent with no contract in place. That is an entity-level exposure, not a branch observation. It goes to the lead auditor immediately.

Code reference: E.4 [SOP600 paras 22, 23]

Q24. My Unit looks like it would be a Significant Data Fiduciary in its own right. Is that my concern?

Yes. Some sub-units handle data of a kind and volume that would attract Significant Data Fiduciary obligations if the unit stood alone, and others do not. You must consider the question and report your assessment to the Lead Enterprise Data Auditor. Clause E.7 also warns against the opposite error — treating a Unit audit as a lesser exercise simply because the Unit sits below the apex.

Code reference: E.7

Q25. My Unit has its own sub-units. Does the SOP apply again, one level down?

Yes, with the necessary changes. If you use the work of a further auditor for a sub-Unit, the same principles apply between you and that auditor, with you acting in the capacity of a Lead Data Auditor for that tier. A branch with sub-branches, or a department with laboratories, is the common case.

Code reference: Section E introduction [SOP600 para 24]

E. Confidentiality, Records and Quality Review

Q26. May I share my working papers with the other auditor?

Yes, to the extent the engagement requires — co-ordination letters, questionnaires, written summaries of procedures and findings are exchanged precisely so the consolidated opinion can rest on something. But the exchange is for that engagement alone.

Note where the duty runs. Each of you owes confidentiality to the audited entity and its Data Principals, not to the other auditor. Neither of you may carry the material into another client, engagement or purpose.

Code reference: C.4 [SOP600 paras 21 to 23]

Q27. How much personal data should pass between auditors?

As little as the audit needs. Prefer pseudonymised or extracted evidence to the underlying personal data, and record what was shared and why. An audit of a consent process usually needs the structure of the consent record, not the names of the Data Principals.

Code reference: C.5

Q28. AIDAI has asked for my working papers. Is producing them a breach of client confidentiality?

No. The obligation to retain the papers and produce them to AIDAI on a quality review or in a disciplinary proceeding is part of the terms on which you hold empanelment, and clause C.6 provides that confidentiality may not be cited to withhold them. The time to deal with this is at engagement, by securing the entity's consent in the engagement terms — which is why the Code asks you to ensure the engagement contract reflects the SOP.

Code reference: C.6 [SOP600 paras 39, 40]

Q29. How long must I keep the papers?

Not less than eight years from the date of the consolidated Data Audit Report, or longer if AIDAI or the DPDPA Rules require it. This applies to the Lead Enterprise Data Auditor and to every Component Data Auditor alike.

Code reference: E.13 [SOP600 para 39]

Q30. AIDAI wants to review an engagement although nobody has complained. Must I co-operate?

Yes. AIDAI may call for and review the working papers of any engagement as part of its quality-review programme, independently of any complaint. Obstructing, delaying or seeking to limit such a review is itself a breach.

Code reference: E.14 [SOP600 para 40]

F. Dealing with Fellow Auditors and the Service Exchange

Q31. I think another empanelled auditor has cut corners. Must I report it?

If you became aware of it while acting as Lead Enterprise Data Auditor or Component Data Auditor, and the departure is of a kind that could affect the reliability of a Data Audit Report, then yes — in writing, to AIDAI, within fifteen days of becoming aware.

Failure to report is itself a breach of the Code. The threshold matters: this is about departures affecting reliability, not about disagreeing with another auditor's style or judgment.

Code reference: F.3 [SOP600 para 33]

Q32. Will I be exposed if I report a fellow auditor?

A report made in good faith is not a breach of confidentiality or of professional courtesy, and no auditor may retaliate against or seek to disadvantage a colleague who makes one. The protection is deliberate: a fifteen-day reporting duty is worthless if reporting carries a professional cost.

Code reference: F.4

Q33. Can the reporting duty be misused against a competitor?

It is meant to be difficult to misuse. A report that is false, frivolous or made for a competitive purpose is itself a breach of the Code, and attracts the same disciplinary process as the conduct it complains of.

Code reference: F.5

Q34. May I tell a client that another auditor's work was poor?

No. Take the disagreement to the auditor concerned and, if it is material, to AIDAI. Clause F.1 prohibits disparaging a fellow auditor's competence or integrity to a client or prospective client, precisely because a genuine professional concern and a competitive manoeuvre look identical from the client's side of the table.

Code reference: F.1

Q35. A Unit is unhappy with its current auditor and has approached me. May I quote?

Not while that engagement subsists. You may not solicit a fellow auditor's engagement in a multi-unit assignment while it is running, nor offer terms calculated to displace an auditor already appointed to a Unit. If the Unit terminates the engagement on its own initiative, that is a different matter.

Code reference: F.2

Q36. How must I describe myself on the AIDAI Service Exchange?

Accurately — empanelment status, accreditation, sectoral competence and capacity. Do not hold out a competence or an availability you do not have. The Service Exchange exists so that Data Fiduciaries can find auditors they can rely on; a listing that overstates competence damages the mechanism for everyone on it.

> **Example.** Listing yourself as available for hospital-sector audits when you have not worked with DGPSI-Hospital is a breach of F.6, and accepting such an engagement would separately breach D.5.

Code reference: F.6; D.5

Q37. I have taken on more component engagements than I can deliver. Can I simply withdraw?

Not in a way that leaves the enterprise audit stranded. An engagement accepted through the Service Exchange is to be performed on the terms accepted; you should not accept work you cannot perform within the timetable, and you may not abandon a component engagement so as to leave the Lead Enterprise Data Auditor unable to complete the consolidated audit.

Code reference: F.7

G. Discipline, Suspension and Grey Areas

Q38. What happens if a complaint is made against me?

A Disciplinary Committee first examines whether the complaint discloses a prima facie case. If it does, you receive a show-cause notice giving you ordinarily not less than fifteen days to respond in writing, identifying the clauses said to have been breached. You may ask for a hearing. The Committee then passes a reasoned order.

The order may close the matter, record an advisory or warning on your file, suspend your empanelment for a specified period, or cancel it. You may appeal to the Governing Council of AIDAI within thirty days, and its decision is final for empanelment purposes.

Code reference: Enforcement 4, 5 [SOP600 paras 34, 36]

Q39. Can I be suspended before the process is complete?

Only where the Disciplinary Committee is satisfied that the matter is serious and that the integrity of the Data Audit process requires it. Interim suspension may not exceed sixty days, reasons must be recorded in writing, and you must be given an opportunity to make a representation within seven days of it taking effect.

Code reference: Enforcement 6 [SOP600 para 38]

Q40. What exactly am I barred from doing while suspended?

Three things. You may not accept a new engagement as Lead Enterprise Data Auditor or Component Data Auditor. You may not hold out as an AIDAI Empanelled Data Auditor in any engagement, proposal, report or Data Trust Score certification. And any Data Audit Report you sign during the suspension will not be recognised by AIDAI as the report of an Empanelled Data Auditor.

Engagements accepted before the suspension are, wherever practicable, handed over to another Empanelled Data Auditor nominated by AIDAI, at your cost. Note that none of this touches any liability you may owe the audited entity under your own contract with it.

Code reference: Enforcement 8; E.12 [SOP600 para 37]

Q41. The situation I face is not covered by any clause. What am I supposed to do?

Work through the decision-making framework: identify the dilemma and who is affected; ask whether the course you are considering aligns with FDPPI's goal of a Secure Information Society; and consult the FDPPI-AIDAI Governance Committee or Advisory Board where needed.

Two additions in this revision matter in practice. If the dilemma is between a lead and a component auditor and cannot be resolved between them, refer it to AIDAI before the consolidated report issues, not after — afterwards there is nothing left to decide. And record the dilemma, the reasoning and the course you adopted in the working papers, so that your judgment can later be reviewed on the basis on which it was actually made rather than reconstructed.

Code reference: Decision-Making Framework 1 to 5

Q42. Where do I confirm my acceptance of the Code?

On the enrolment application, and again on each renewal by the undertaking prescribed under the SOP. AIDAI also makes available a draft contract of engagement; auditors accepting a lead or component role should ensure their engagement terms reflect the SOP's requirements on co-ordination, the standard communication procedure, eight-year retention of working papers and their production to AIDAI.

Code reference: Acceptance and Engagement Terms; A.5

Referring a Question

Questions on the interpretation of this Code, or on a situation it does not clearly cover, may be referred to the FDPPI-AIDAI Governance Committee or Advisory Board. Where a referral concerns a live engagement, make it before the Data Audit Report is issued.