

Sovereign AI is a control question, not a location question.

A submission to the consultation "**Getting it right: Building AI infrastructure that works for Australia**", Department of the Prime Minister and Cabinet. **Katonic AI**. Lodged 2 October 2026 by Prem Naraindas, Founder and Chief Executive. Contact details are provided through the submission form. Katonic AI consents to this submission being published.

1 What we ask

We ask that Australia's AI Standards prescribe a one-page Control Disclosure, and require it from every supplier of an AI service to a Commonwealth entity or a critical infrastructure operator, wherever the service is hosted. For four controls, the disclosure names which party holds each one and under whose law: the keys to the data, the choice of model, the record of what the system does, and the power to switch it off. The law would require a true answer, not a particular one. The paper's 58 questions cover the buildings, the grid, the water, the communities and the laboratories. None asks who controls the AI systems that Australian organisations will run on that infrastructure. Location is necessary. It does not settle control.

2 Who we are, and our interest

Katonic AI is an Australian company, founded in Sydney in 2020, with offices in Sydney, Mumbai and Dubai, where its founder is based. Our platform is installed inside the customer's own environment, in its data centre or its own cloud tenancy. It serves enterprise customers in eleven countries, including Pilipinas AI, the sovereign AI service run with ePLDT in the Philippines, and MODON, the Saudi industrial cities authority. We develop no models of our own, and we are certified to ISO/IEC 27001:2022. Our interest is direct: we sell a platform to which this disclosure would apply. Installed software answers some of these questions more easily than a hosted service, which suits us. That is why every question applies to every layer, including ours.

3 The gap in the paper

The paper makes onshore infrastructure a precondition: sovereign AI capability, it says, "relies on secure, onshore data centre infrastructure". It also warns that Australia "risks hosting AI infrastructure and training activity while the associated research outputs, model development, intellectual property and commercial returns accrue offshore". Control is the same risk one layer down. The paper defines a "data centre user" as "a person who uses compute supplied by a data centre" and attaches nothing to that user. Yet that is where the exposure sits. A hospital, a bank or an agency can run an AI system in a certified Sydney facility while a supplier abroad holds the keys, changes the model without notice, keeps the only record of what the system did, and can end the service. That is a well-located dependency, not sovereign capability.

Existing law points at the gap without closing it. Foreign-investment screening governs who may own a facility or a business. Rules made in June 2026 under the Security of Critical Infrastructure Act will require operators in nine critical infrastructure classes, including electricity, gas and water, to assess the foreign ownership, control or influence risks of their major suppliers, from 2027 and 2028. APRA's CPS 230 requires banks, insurers and superannuation trustees to manage their material service providers, including core technology providers. Each duty falls on the buyer, and none gives the buyer a common form in which a supplier answers. Part 3's conditions bind the laboratories that train frontier models. They do not reach the systems Australian organisations deploy, which is where most of the country's AI will run.

4 The four controls

Each answer names a party, not an assurance. Every party that hosts, runs or supplies part of the service answers: the cloud or facility operator, the platform supplier and the model developer. Each also states its ultimate owner, where it and anyone with access to the hardware or data are based, and which countries' laws can compel it to disclose the data, change the system or stop it.

1 Keys

Who holds the keys to the data, and can any supplier obtain a copy? Where is the data decrypted for processing, on whose hardware, and may anyone train a model on it?

2 Models

Who chooses which models run, who developed them and under what licence, and who decides when they change?

3 Evidence

When the system acts, including when it refuses, what record is kept, where, and who can read it? How soon is the customer told of an incident?

4 Switch-off

Who can stop the system, and does it keep running if a supplier's service or licence ends?

The attached draft form gives each question a graded set of answers, strongest first. A weak answer is not a ban. A buyer may accept one knowingly, and the disclosure makes sure it knows.

5 Three worked examples, all hypothetical

An Australian insurer runs an AI system in its own tenancy on a foreign-owned public cloud. It holds the keys in a store the cloud provider does not operate, approves each model change, and keeps the full record in its own environment. Its platform supplier answers "the insurer" four times. The cloud provider's disclosure names the foreign law that can compel it, and the insurer keeps running if that cloud's service ends only if it has a tested way to leave.

A state agency subscribes to an AI service in a certified Sydney data centre. The vendor holds the keys, changes the model on its own schedule, keeps the record on its side, and ends the service when the subscription ends. Every answer names the vendor, on Australian soil, in a facility that would meet every requirement in the paper.

Installed software can fail too. Ours stops when its licence ends, which leaves us holding an off switch inside the customer's own data centre. The disclosure would make us say so, as it would any supplier.

The four questions do not repeat the paper's location test. They add what it leaves out: who can switch the system off, and under whose law.

6 Where it fits, with proposed wording

Question 49 offers "an obligation to publish in a specified form". Proposed wording: "A person who contracts to supply an AI service to a covered user must, before supply, give the covered user and the regulator a Control Disclosure in the approved form, obtain the answers from every party upstream, update it within 30 days of any change that makes it inaccurate, and publish a summary. A covered user must not use an AI service without a current Control Disclosure. A covered user is a Commonwealth entity, or a responsible entity under the Security of Critical Infrastructure Act in relation to its asset." The form belongs in rules rather than in the Act, so it can move with the technology. A knowingly or recklessly false answer should attract a civil penalty. A developer authorised under Part 3 would give a Control Disclosure for each AI service it supplies to a covered user.

Question 50, on safeguards: the full disclosure goes to the customer and the regulator, and only a summary is published, so the register is not a map of who can switch off critical systems.

Question 57, on existing law: one form, reused, would serve duties already made, all Commonwealth: the SOCI risk management rules, CPS 230, and the Privacy Act's requirement, from 10 December 2026, to disclose in privacy policies the kinds of automated decisions that significantly affect individuals and the personal information they use. It could also serve the reform of the Hosting Certification Framework.

Questions 1 and 2, on thresholds: do not tier the disclosure by megawatts. The smallest deployment can carry the largest dependency, and every answer is a fact a supplier already knows about its own service.

7 Precedent

The Commonwealth already grades hosting by control as well as by address. Under the Hosting Certification Framework, now being reformed, Certified Strategic status "is only available to Service Providers that allow the government to specify ownership and control conditions", and the framework exists to give "greater assurance over the ownership, control, operations and supply chains of Service Providers". We propose the same logic one layer up, for AI services. In August 2026 the Australian Signals Directorate and the Australian Institute of Company Directors told boards to "assess the risk of relying on AI providers, including cyber supply chain risks and concerns about foreign ownership, control and influence". A Control Disclosure is the document that assessment needs.

8 In closing

We would welcome the chance to discuss the attached draft form with the Office of AI. The four questions are short enough to answer on one page and specific enough that a weak answer shows, which is what makes them worth asking.

ANNEX A

Draft Control Disclosure

One page per AI service. Every party in the chain answers. The published summary shows Parts 1 and 3, with answer letters only.

Part 1. The service. Service name and version. Covered user. Date. The version it replaces, and what changed.

Part 2. The parties. One row for each party that hosts, runs or supplies part of the service: the cloud or facility operator, the platform supplier, each model developer, and any sub-processor with access to the data. For each: name; place of incorporation; ultimate owner; the countries where it, or anyone with access to the hardware or data, is based; the countries whose law can compel it to disclose the data, change the system or stop it.

Part 3. The four controls. For each control, tick the answer that is true and name the party.

CONTROL	A (STRONGEST)	B	C	ALSO STATE
Keys	the customer holds the keys in a store no supplier operates, and no supplier can obtain a copy.	the customer holds the keys in a store a supplier operates.	a supplier holds the keys or can obtain a copy.	Also state where the data is decrypted for processing and on whose hardware, and whether any party may train a model on it.
Models	the customer chooses each model, approves each change before it takes effect and can keep any approved version, with urgent security fixes applied first and notified when made.	the customer is told a stated number of days before a change, can decline it for a stated period, and keeps the prior version while it retests.	a supplier changes models without notice.	Also state each model's developer and licence.
Evidence	every action, including refusals, is recorded in the customer's environment, and the customer sets retention and controls access.	a supplier holds the record, and the customer can obtain a full copy within a stated number of days.	the customer cannot obtain a full record.	Also state every party that can read the record, and the incident-notice period in hours.
Switch-off	the customer can stop the system without any supplier, and it keeps running if any supplier's service or licence ends.	the customer can stop it, and when a supplier's service or licence ends it keeps running for a stated period, or the customer can leave with its data, models and configuration under a tested exit plan.	the service stops when a supplier's service or licence ends.	

Part 4. Sign-off. Approved by the supplier's board or a named officer. The published summary shows Parts 1 and 3, with answer letters only.