AI agents inside government

What they can read, what they can reach, and who decides

IN BRIEF

01 Governments have moved from asking whether to use AI to counting how many officers already do. Singapore told its parliament that about 80 percent of its 150,000 officers have used the government's general chatbot. The United Kingdom's question-answering service for citizens raised its accuracy from 76 to 90 percent across two public pilots before launch. The United Arab Emirates has named its first four agents for federal work, among them procurement and tax audit.

02 Three things are still missing in most of what has been published. Few bodies say where the agent runs. Almost none says who approves what the agent produces. And the work inside the building, the drafting, checking and preparing that fills an officer's day, has no ready-made agent in any library we could find.

03 This paper is about that work. It sets out what an agent inside a government body can read, how it reaches the systems of record, what it may do without a person, and what the rules in our markets already ask. It ends with seven questions to put to any supplier, and with a place to start.

04 The position throughout is simple. An agent prepares. A named officer decides. The agent runs on infrastructure the body controls.

IN THIS PAPER

01 Where governments are today 2
02 The work nobody has packaged 3
03 Three doors, one gate 4
04 What an agent may do 6
05 What the rules already ask 6
06 A worked example: a revenue directorate 8
07 Seven questions before an agent touches a case 9
08 Where to start 9

PART 01

Where governments are today

About 80%

of Singapore's 150,000 public officers had used the general chatbot

76 to 90%

accuracy of the United Kingdom's question-answering service, rising over two pilots

4

agents announced by the UAE's federal government in May 2026

25

councils in the United Kingdom joined the trial of a tool that turns meetings into notes

Staff assistants are the largest use. Singapore's Ministry of Digital Development and Information told parliament in November 2025 that about 80 percent of 150,000 public officers had used the general chatbot, and that officers had built more than 20,000 chatbots of their own on internal data [1]. Malaysia piloted a writing and meeting assistant with 270 officers before offering it to up to 445,000; the supplier reported that 97 percent of the pilot group saved 3.25 hours a week each [2]. France's Ministry of Economy and Finance runs assistants on its own premises for 10,000 employees; its supplier reports document retrieval cut from two days to two minutes [3].

Citizen services come next, and they are measured in public. The United Kingdom launched a question-answering service in its government app in May 2026. More than 7,800 people had used it at launch, and its own account says it "does not attempt to provide advice" [4]. Its builders reported accuracy rising from 76 to 90 percent over two pilots, and 508 attempts to make it answer harmfully [5]. Abu Dhabi's government reports more than 1.9 million service cases completed through conversational AI [6].

Agents that act are arriving. The UAE's federal government announced four agents in May 2026: procurement support, tax audit data checks, information for service staff, and technical support [7]. Singapore is building a registry of agents and their owners for its 150,000 officers, with controls that can stop an agent deleting files or sending email outside government [8].

Small, useful tools are spreading faster than large ones. In the United Kingdom, 25 councils joined the trial of a tool that turns meetings into notes. In earlier central government tests it saved an hour of administration for each hour of meeting [9].

What the published accounts leave out. Of the government deployments we read, a handful state where the agent runs: the French ministry on its own premises, a German state in a sovereign national cloud, Abu Dhabi in a sovereign cloud. Most say nothing. And a step where a person approves the output is almost never described. Those two silences are where a buyer should press.

Not every pilot survives. New Zealand's chatbot for businesses launched in September 2024 and was withdrawn within months [10].

A pilot that depends on a supplier's hosted service, with no owner inside the body, ends when the pilot budget does.

PART 02

The work nobody has packaged

23 of 55

jobs done inside government bodies appear in none of the template libraries

2

of the templates we opened put an approval before the output went out

We listed 55 jobs done inside government bodies and looked for each one in the template libraries of the agent and workflow platforms. Twenty-three appear in none.

WHERE TEMPLATES EXIST	WHERE NONE WAS FOUND
Answering citizens' questions from published pages	**Checking a planning application against zoning rules**
One permit intake flow	**Preparing a tax return for an auditor's review**
Screening benefit claims for fraud risk	**Drafting a reply to a citizen's letter**
Finding records for an information request	**Preparing an appeal bundle**
Screening grant applications	**Setting tender bids against the published criteria**
Staff questions on HR policy	**Analysing responses to a public consultation**
	Minutes of a meeting
	Applying a records retention schedule

The pattern is consistent. Templates exist for the front counter. They do not exist for the work behind it, which is where most officers spend most of their time, and which governments are now building for themselves: the United Kingdom's consultation and minutes tools were built by government, not bought.

Two more findings matter to a public body. Where a template exists, it rarely holds a step for a person: of the templates we opened, two put an approval before the output went out, and in one of those the AI could still refuse an application by itself.

And most lean on a public cloud mail, spreadsheet or model service, which settles the data question before the body has asked it.

PART 03

Three doors, one gate

An agent is only as useful as what it can reach. In a government body that means three kinds of thing.

Documents.

Legislation, circulars, rulings, programme rules, the correspondence standard, internal policy. These are indexed once as knowledge sources, with each reader's permissions kept, so an agent answers with the section it relied on and says when the documents are silent.

Systems of record.

The case system, the register, filings, payments. Most are reached through an interface the body already runs. The body gives the platform the description of that interface, chooses which operations become tools, and decides which of them need approval.

Data for analysis.

Reporting databases, read only.

All three pass one gate: every tool call is checked against the body's policy, which can allow it, record it, hold it for a person, or block it.

SIX WAYS INTO A GOVERNMENT BODY'S SYSTEMS

	ROUTE	WHAT IT REACHES	WHAT TO KNOW
01	**A file the officer uploads**	An application, a letter, a bid, a recording	Nothing is connected. The safest start
02	**A knowledge source**	Law, rules, policies, past rulings	Permissions are kept per reader
03	**An imported description of your own interface**	Case system, register, filings	You choose the operations. Changes wait for approval
04	**A national exchange layer**	Other bodies' registers	The exchange's own sign-in and logging still apply
05	**A server from the tool catalogue, run in your cluster**	Databases, search, document conversion	It runs inside; check what each tool does
06	**A supplier's own tool server**	A supplier's case or service system	Few exist for permitting, tax or records systems

PART 03 · CONTINUED

18
interface descriptions taken from their publishers' own addresses; the importer accepted all 18

853
operations the importer found in them

5 of 18
files ask for an OAuth 2 sign-in

143
operations that change something in two administration files

What is published. Governments publish more interface descriptions than most industries. We took 18 from their publishers' own addresses, among them the United Kingdom's tax authority and payment service, Estonia's data exchange software, the European Union's public procurement notices, and Australia's statistics office, and gave them to the platform's importer. It accepted all 18 and found 853 operations. Some national platforms publish no description at all, among them the sign-in services of Singapore and the UAE. There the body supplies its own.

What that exercise taught us. Five of the 18 files ask for an OAuth 2 sign-in, one of them in the form where a system proves its identity with its own credentials, and several national sign-in services ask for a token signed with a private key. A large file can carry far more than a team needs: two administration files carried 143 operations that change something, where a team reading its own cases needs perhaps a dozen. So choose the operations at import, and import nothing that changes a record until the approval step has been seen working.

Supplier tool servers. Two large service-management suppliers published tool servers for agents in 2026. For the permitting, tax and records systems that most bodies run, we found none.

The dependable routes are the body's own interface and its own database.

PART 04

What an agent may do

One rule runs through every agent in this paper: it prepares, and a named officer decides.

01	**It reads** what the officer could read, and no more.
02	**It drafts** the note, the letter, the schedule, the comparison, with each statement tied to its source.
03	**It lists** what is missing, what does not match, what departs from the rule.
04	**It stops** before anything that changes a record or reaches a citizen. A tool that changes something waits for approval.
05	**It decides nothing about a person.** It does not grant or refuse a benefit, a permit or a refund, select a taxpayer for audit, score a bid, or release a record.

This is not caution for its own sake. It is the line the rules draw, as the next part shows, and it is the line that two governments crossed at great cost. In the Netherlands, a court struck down a welfare fraud risk system in 2020 because its use was “insufficiently transparent and verifiable” [11]. In Australia, a royal commission into an automated debt scheme recommended more review and oversight of automated decisions, and the government has consulted on a framework to deliver it [12].

PART 05

What the rules already ask

This part needs a lawyer’s read before it is relied on. It reports what the texts say; it is not advice.

Three documents written for agents

Singapore. The Infocomm Media Development Authority’s framework for agentic AI (version 1.5, May 2026) says “human responsibility continues to apply”, asks organisations to “define significant checkpoints or action boundaries that require human approval”, and names sending communications and making payments as actions that cannot be undone [13]. Singapore’s own government technology controls go further on location: for confidential data, “use only services served by models hosted in Singapore”, and a body that hosts its own model must use an environment cleared for the highest classification the model will process [14].

United Kingdom. The government’s AI Playbook has a section on agentic AI and a principle titled “You have meaningful human control at the right stages”. Where a service affects a person’s rights, a body “must only use AI to support decisions that must be made by a human decision maker” [15].

PART 05 · CONTINUED

What applies to every AI system

European Union. The AI Act lists as high-risk any system public authorities use "to evaluate the eligibility of natural persons for essential public assistance benefits and services" [16]. A public body that deploys one must assign oversight to people with "the necessary competence, training and authority", carry out a fundamental rights impact assessment, register the use, and keep the system's logs. A regulation of July 2026 moved the date these duties apply to 2 December 2027 [17]. Separately, the data protection regulation gives a person the right not to be subject to a decision "based solely on automated processing" [18].

United Kingdom. Central government must publish a record for any algorithmic tool that has "a significant influence on a decision-making process with public effect" or that deals directly with the public [19].

Market by market

MARKET	WHAT WE READ	WHAT IT ASKS
European Union	AI Act, as amended in July 2026; data protection regulation	Oversight by trained people, impact assessment, registration, logs; high-risk duties from 2 December 2027
United Kingdom	AI Playbook; transparency recording standard	A human decision maker where rights are affected; a published record
Singapore	Agentic AI framework; government technology controls	Approval checkpoints; confidential data only on models hosted in Singapore
United Arab Emirates	National AI charter (2024)	Human oversight and accountability as principles; no location rule found in it
Saudi Arabia	Draft responsible AI policy (2026), read in a law firm's summary	Human supervision where people are affected; registration of government AI
India	AI governance guidelines; data protection rules (2025)	Meaningful human control; standards and logs for processing by the State
Australia	Policy for responsible use of AI in government, version 2.0, read in summary	Accountable officials, a register of uses, a public transparency statement
New Zealand	Public service AI framework	Human oversight, explainable outcomes, auditing

We did not open a government-use rule for Qatar, Malaysia, Indonesia, the Philippines or Thailand, and for Australia and Saudi Arabia we read summaries and not the primary text. A body in those markets should ask its own counsel.

PART 05 · CONTINUED

What the rules have in common

Read together, the texts ask four things of an agent in a public body, and all four are matters of how the system is built:

01	**A person decides** wherever a citizen's rights or money are affected.
02	**The citizen can be told** that AI was used, and the use can be put on a register.
03	**The body knows where the data is processed,** and for sensitive data that is in-country or on its own infrastructure.
04	**There is a record** of what the agent did, kept long enough to answer a complaint or an audit.

PART 06

A worked example: a revenue directorate

In October 2026 we built four agents for an invented revenue directorate, on invented law and invented case files, to show the pattern end to end.

AGENT 01

A rulings assistant for officers. Asked which circular governs electronic invoicing for small traders, it names the current circular, says which one it replaced and under which section, and gives the date small traders come into scope. Asked something the documents do not cover, it says so.

AGENT 02

A case analyst. It finds that three open cases share a director or an address, names each case it relies on, and when asked about a case number that does not exist it says there is no such case.

AGENT 03

A letter agent. It rewrites a dense penalty notice to the directorate's plain-language standard. Every amount, date and legal reference survives; the director's personal email, telephone number and identity number do not. A named reviewer approves the letter.

AGENT 04

A taxpayer assistant on the directorate's website. It has the rules and not the records. Asked about another company's case, it refuses and says why.

For an officer working one case, the same agent reads the taxpayer's filings from the directorate's case system through an imported description of that system's interface, works out the exposure under the act, and drafts a case note. The note is written to the case system only after an officer approves it.

Nothing in this example is a customer's data, and the directorate does not exist. The documents, the mock case system and the expected answers are available to any body that wants to repeat it on its own infrastructure.

PART 07

Seven questions before an agent touches a case

01 **Where does it run?**
On our infrastructure, in a cloud region in our country, or in the supplier's service? Where is the model?

02 **What can it read?**
Does it keep each officer's permissions, or does it read as one all-seeing account?

03 **What can it change?**
Which tools write to a record or send something, and does each wait for a person?

04 **Who decides?**
Show us the step where a named officer approves, and what the agent does when nobody has.

05 **What is recorded?**
Who asked, which tool ran, what was decided, and for how long is that kept?

06 **Can we tell the citizen?**
Is there enough on record to say AI was used, to explain its part, and to enter the use on a register?

07 **Can we stop it?**
One agent, one tool, or all of them, at once, by us.

PART 08

Where to start

Pick work where reading is slow, the decision stays with an officer, and no citizen is waiting on the agent.

Questions on your own law and rules

Officers ask what the legislation and the circulars say and get the answer with the section cited. No citizen data is involved, so it can run on the first day.

Letters in plain language

The agent rewrites a notice to your own correspondence standard and keeps every amount and date. A named reviewer approves each one.

Consultation responses

The agent groups the responses and quotes the ones behind each theme. Policy staff check and conclude.

One team, one programme, invented data first. Then beside the manual process, measured against it.

About Katonic AI

Katonic AI builds the platform that organisations use to build, run and govern AI agents on their own infrastructure: in their own data centre, in a sovereign cloud, or with no connection to the internet at all. The platform is in production with governments, banks, telecom operators and utilities. Katonic is certified to ISO 27001.

KATONIC.AI

SOURCES

Read on 21 November 2026. Figures are the publishers' own and were not audited by us.

01 Ministry of Digital Development and Information, Singapore, reply to a parliamentary question on AI tools in the public service, 6 November 2025. mddi.gov.sg

02 Google Cloud press release, "445,000 Public Officers in Malaysia to Benefit from Generative AI", 5 February 2025. googlecloudpresscorner.com

03 NVIDIA case study on ThinkDeep and the French public administration (supplier's figures). nvidia.com/fr-fr/case-studies

04 Government Digital Service, "GOV.UK Chat launches", 14 May 2026. gds.blog.gov.uk

05 The Register, 19 March 2026, reporting the Government Digital Service's pilot results. theregister.com

06 Apolitical case study of TAMM, citing the Abu Dhabi Department of Government Enablement's 2025 review, January 2026. apolitical.co

07 The National, "UAE launches first batch of AI agents", 20 May 2026. thenationalnews.com

08 The Star, citing The Straits Times, "Singapore to create a registry of AI agents for 150,000 public officers", 2 June 2026. thestar.com.my

09 UK Government news, "AI experiments see Humphrey help townhalls cut costs and improve services", 23 May 2025. gov.uk

10 Interest.co.nz, on the end of the GovGPT pilot, February 2025. interest.co.nz

11 The Hague District Court, press release on the SyRI judgment, February 2020. rechtspraak.nl

12 Attorney-General's Department, Australia, "Automated Decision-Making Reform" consultation, on recommendation 17.1 of the Royal Commission into the Robodebt Scheme. consultations.ag.gov.au

13 Infocomm Media Development Authority, Singapore, Model AI Governance Framework for Agentic AI, version 1.5, 20 May 2026. imda.gov.sg

14 Government of Singapore, ICT and Smart Systems policy, generative AI controls GA-9 and GA-11. info.standards.tech.gov.sg

15 UK Government, Artificial Intelligence Playbook for the UK Government, 10 February 2025. gov.uk

16 Regulation (EU) 2024/1689 (AI Act), Annex III point 5(a); Articles 14, 26, 27 and 49.

17 Regulation (EU) 2026/1744, Official Journal 24 July 2026.

18 Regulation (EU) 2016/679, Article 22.

19 UK Government, Algorithmic Transparency Recording Standard: mandatory scope and exemptions policy, 17 December 2024. gov.uk

20 Template libraries of agent and workflow platforms, searched 21 November 2026; and 18 interface descriptions fetched from government publishers the same day (Katonic research).