

Seven things every business must do before December as AI governance rules kick in - blueAPACHE

Canonical: <https://www.blueapache.com/blog/seven-things-every-business-must-do-before-december-as-ai-governance-rules-kick-in>

Details:

Summary

This blueAPACHE post reports: From 10 December 2026, Australian businesses must disclose how AI influences decisions about people or face fines up to \$50 million. AI agents are already reading your files, sending emails, and making workflow decisions without a human in the loop. It concerns Governance, Risk & Compliance, emPOWER Security, Microsoft Practice. It names Microsoft, Gartner in connection with the announcement. Published in 2026. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2026
Services referenced	Governance, Risk & Compliance, emPOWER Security, Microsoft Practice
Named products or vendors	Microsoft, Gartner
Cited figure	...how AI influences decisions about people or face fines up to \$50 million. AI agents are already reading your files, sending emails, and...

Article

From 10 December 2026, Australian businesses must disclose how AI influences decisions about people or face fines up to \$50 million. AI agents are already reading your files, sending emails, and making workflow decisions without a human in the loop. A major Privacy Act deadline is now only six months away, and most organisations are nowhere near ready. Less than a year ago, the biggest risk most businesses worried about was an employee pasting sensitive data into ChatGPT. While that is still an issue, it's no longer the primary concern. In the first months of 2026, AI has moved from generating content to acting autonomously. The tools your teams are adopting are reading your SharePoint files, updating your CRMs, and executing multi-step workflows without anyone clicking 'approve'. At the same time, a critical regulatory deadline is approaching that will make governance obligations legally enforceable for the first time, and many organisations don't even know it is coming.

The December deadline you need in your diary

From 10 December 2026, amendments to Australia's Privacy Act will mandate transparency obligations on any organisation using automated decision-making (AI) that could significantly affect individuals' rights or interests. If your organisation uses AI systems to influence decisions about hiring, lending, insurance, customer access, or service delivery, you will need to clearly disclose it in your privacy policy, including the types of personal information used and the types of decisions being made. The Office of the Australian Information Commissioner (OAIC) has already commenced its first privacy compliance sweep this year across 60 businesses in high-risk sectors. Non-compliance could attract civil penalties of up to \$66,000 per offence, with serious breaches carrying fines of up to \$50 million or 30 per cent of annual turnover. Meanwhile, Australia's AI Safety Institute started operating in early 2026 with \$29.9 million in funding, and the Senate Select Committee on Adopting AI has released a consultation paper on proposed mandatory guardrails for high-risk AI applications.

Shadow AI has evolved and it is bigger than we think

Before getting to the list of seven things organisations should be doing to prepare, I want to set the scene around the scale of the problem Australia faces. Shadow AI is when employees use AI tools at work without their employer's approval or oversight, putting company data and client information at risk because there's no visibility over where it's going or how it's being used. Microsoft's 2026 Data Security Index reinforces just how widespread the problem already is, with more than 70 per cent of employees bringing their own AI tools into work, often through personal accounts that bypass corporate controls. The same Microsoft research found GenAI was involved in 32 per cent of data security incidents over the past year. Shadow IT used to mean someone putting a company spreadsheet in a personal Dropbox. Today its evolution into "Shadow AI" means staff are sending intellectual property into models that can retain it, learn from it, and potentially share it. The risk surface is also expanding rapidly. Gartner predicts that 40 per cent of enterprise applications will be integrated with task-specific AI agents by the end of 2026, up from less than 5 per cent in 2025, dramatically widening the exposure for any organisation without governance in place. Yet Microsoft's research shows just 47 per cent of organisations have implemented GenAI controls, leaving a significant gap between adoption speed and governance maturity.

Seven things every Australian organisation should be doing now

****Audit your AI exposure now** ****Map every AI tool being used across your organisation, including the unauthorised ones.** Identify which systems touch personal information and which are influencing decisions about individuals. This is the baseline for Privacy Act compliance and key to understanding where your real risk lies.

****Update your Acceptable Use Policy for AI specifically** ****A policy drafted a year ago is already outdated.** A modern AI AUP needs to go beyond 'do not paste confidential data into ChatGPT.' It should specify which tools are approved, what data classification levels each can process, where data is stored and whether it leaves Australian jurisdiction, as well as what employees are responsible for when using AI-generated outputs. Be sure to address any unsanctioned tools your people are more than likely using.

****Put explicit controls around agentic AI** ****If you are using AI agents that can take actions across your systems, reading files, executing workflows, interacting with other tools, you need guidelines that specifically address that.** Give agents the minimum level of access they need to do their job (principle of least privilege), and ensure mandatory human approval at critical decision points, real time behavioural monitoring, and comprehensive logging of every action an agent takes. Treat your AI agents like you would a new hire with administrator access.

****Embed human oversight into high-stakes decisions** ****AI is a capable co-pilot, but a real person must be accountable for the final call.** Good governance means maintaining human-in-the-loop controls for any decision that carries material business, legal, or reputational risk. It is not only good practice, it is

becoming a regulatory expectation. Under the coming Privacy Act amendments, showing meaningful human oversight will be a factor in how automated decision-making obligations are assessed.

****Vet your AI supply chain ****The AI supply chain has become a target for attack. Your governance framework should include proper due diligence on every AI tool and third-party framework before it is deployed. If a vendor cannot tell you where your data goes, what it is used for, and how long it is retained, then walk away.

****Build ongoing risk assessment into your governance cycle ****Regular risk assessments, penetration testing of AI systems, and compliance audits should be a standing part of your governance calendar. The threat landscape in this space is moving faster than almost any other area of cybersecurity, and a review conducted 12 months ago probably already has gaps.

****Bring in specialist expertise if you need it ****AI governance straddles cybersecurity, legal compliance, and operational risk. If your internal team is not across the incoming Privacy Act obligations, the agentic AI threat landscape, and what a modern Acceptable Use Policy actually needs to cover, the cost of getting it wrong will be a lot more than the cost of engaging outside help.

An experienced consultant who works in this space daily will compress months of internal effort into weeks and is far less likely to leave critical gaps. Your employees are already using AI tools, regardless of whether you approved the usage or not. Now, it is up to you to make sure your organisation has the controls, and policies to manage that adoption securely, responsibly, and legally. With Australia's Privacy Act changes coming out in December, time is running out to be on the front foot. [Click here to read the full article.](#)

Related

Governance, Risk & Compliance

emPOWER Security

emPOWER Security (pillar)

Microsoft Practice (pillar)

Frequently asked questions

What is the December 2026 Privacy Act deadline described in the article, and what penalties does it carry?

From 10 December 2026, amendments to Australia's Privacy Act require organisations using automated decision-making that could significantly affect individuals' rights to disclose it in their privacy policy; non-compliance can attract civil penalties up to \$66,000 per offence, with serious breaches carrying fines up to \$50 million or 30 percent of annual turnover.

What Microsoft research figures does the article cite on shadow AI and GenAI-related incidents?

The article cites Microsoft's 2026 Data Security Index finding that more than 70 percent of employees bring their own AI tools into work through personal accounts, that GenAI was involved in 32 percent of data security incidents in the past year, and that only 47 percent of organisations have implemented GenAI controls.

What does the article say the OAIC has already begun doing in 2026?

The article says the Office of the Australian Information Commissioner has commenced its first privacy compliance sweep in 2026 across 60 businesses in high-risk sectors.

What are the seven things the article recommends businesses do to prepare?

The article recommends auditing AI exposure, updating the Acceptable Use Policy for AI specifically, putting explicit controls around agentic AI, embedding human oversight into high-stakes decisions,

vetting the AI supply chain, building ongoing risk assessment into governance, and bringing in specialist expertise where needed.

Is the information in this post still current?

This reports the automated decision-making deadline and figures as understood earlier in 2026; because the deadline falls on 10 December 2026, readers should confirm final requirements directly with the Office of the Australian Information Commissioner rather than relying solely on this post.

Source

<https://www.blueapache.com/blog/seven-things-every-business-must-do-before-december-as-ai-governance-rules-kick-in/>

Knowledge Base

From what date must Australian businesses disclose how AI influences decisions about people, and what is at stake for non-compliance?

From 10 December 2026, Australian businesses must disclose how AI influences decisions about people or face fines up to \$50 million.

What do the December 2026 Privacy Act amendments require of organisations using automated decision-making?

Amendments to Australia's Privacy Act will mandate transparency obligations on any organisation using automated decision-making (AI) that could significantly affect individuals' rights or interests. Organisations using AI to influence decisions about hiring, lending, insurance, customer access, or service delivery must clearly disclose this in their privacy policy, including the types of personal information used and the types of decisions being made.

What penalties can businesses face for non-compliance with the new Privacy Act obligations?

Non-compliance could attract civil penalties of up to \$66,000 per offence, with serious breaches carrying fines of up to \$50 million or 30 per cent of annual turnover.

Has the OAIC already begun enforcing privacy compliance related to AI, ?

Yes, the Office of the Australian Information Commissioner (OAIC) has already commenced its first privacy compliance sweep this year across 60 businesses in high-risk sectors.

What is 'Shadow AI' and how widespread is it according to Microsoft's 2026 Data Security Index?

Shadow AI is when employees use AI tools at work without their employer's approval or oversight, putting company data and client information at risk because there's no visibility over where it's going or how it's being used. Microsoft's 2026 Data Security Index found that more than 70 per cent of employees bring their own AI tools into work, often through personal accounts that bypass corporate controls, and GenAI was involved in 32 per cent of data security incidents over the past year.

What does Gartner predict about AI agent integration in enterprise applications by the end of 2026?

Gartner predicts that 40 per cent of enterprise applications will be integrated with task-specific AI agents by the end of 2026, up from less than 5 per cent in 2025, dramatically widening the exposure for any organisation without governance in place.