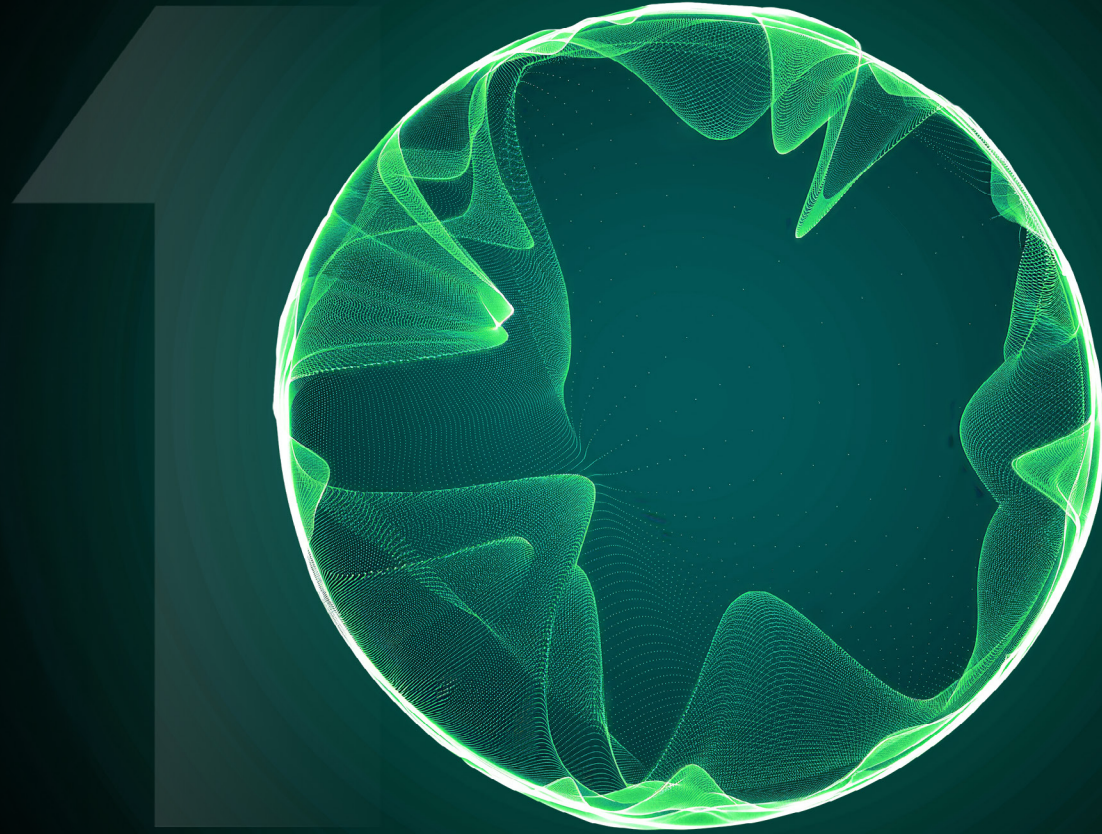


Deloitte.



A Transparent Tomorrow

Deloitte Australia Privacy Index 2024

10th edition

Contents

Foreword	03
About the report	04
Key findings	05
Privacy Index 2024	07
Consumer Index 2024	08
No regrets moves	10
<i>Chapter 1</i>	
The privacy pitfall	
The innovation race leaving customers behind	11
<i>Chapter 2</i>	
Upgrade required	
Getting with the (privacy) program	17
<i>Chapter 3</i>	
Privacy bootcamp	
It's time for a glow-up	20

Foreword

Do you remember your first online purchase? AI does. Can you recall every social media comment you've made? AI can. Lost track of all your taxi rides? Not AI – it knows exactly where and when you went.

Our lives are increasingly intertwined with technology that tracks every purchase, monitors every click, and remembers every interaction. This personal information is often used to make important decisions about us, such as home loans, shopping recommendations, and job applications through data and artificial intelligence (AI) algorithms that often lack human oversight.

This raises serious concerns about:

- Privacy risks
- Bias and discrimination
- Echo chambers
- Data security
- Lack of accountability
- Insufficient transparency
- Ethical data use
- Loss of consumer autonomy
- Digital inequality
- Informed consent
- Regulatory compliance
- Lack of user control

How does that make you feel?

The rapid adoption of technologies like AI, generative AI (Gen AI), and automated-decision making (ADM) is revolutionising industries across Australia. Yet, with this progress comes a critical responsibility: ensuring personal information is handled with transparency and integrity.

In this year's Privacy Index, we studied the AI management practices of Australia's leading brands to see if they prioritise consumers or if their privacy practices are lagging. We also surveyed consumers to understand their perceptions of how organisations have managed the transition to these technologies and whether the trust gap has narrowed or widened.

For organisations, bringing consumers on the journey, giving them a voice, and providing a clear understanding of data usage is crucial to the adoption and future success of innovative technology, and business.

By fostering a future where technology and trust go hand in hand, we can ensure that innovation serves everyone responsibly, enhancing lives while respecting privacy.

The Privacy Index 2024 is a powerful tool to help you understand why transparency and trust are key to future business success and how to implement best practices for data protection and ethical AI use.

Remember, this doesn't just affect your organisation – it affects *your* life too.



Daniella Kafouris
Partner, Technology & Transformation



Lucy Mannering
Partner, Technology & Transformation



About the report

The future of privacy in the age of intelligent automation

As we enter the age of intelligent automation, where innovative technology, such as AI, Gen AI and ADM, is increasingly used to make decisions impacting our lives, what does it mean for the future of privacy and trust?

In this year's Privacy Index, we address this crucial question by examining AI and ADM management practices across 10 key Australian industries. We analyse whether current privacy practices can withstand future technological advancements and the upcoming Australian privacy reforms – the most significant since 2014. Additionally, we survey Australian consumers to understand their opinions and expectations.

Our comprehensive report gives organisations valuable data-driven recommendations and actionable insights, while giving consumers a deeper understanding of privacy.

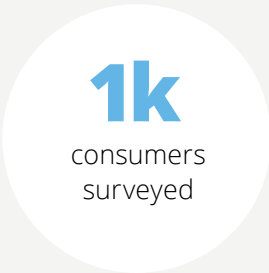
AI terms

- AI:** the simulation of human intelligence processes by machines, especially computer systems.
- Gen AI:** a subset of AI that focuses on creating new content, such as text, images, music or code, by learning patterns from existing data.
- ADM:** the use of algorithms and AI to make decisions without human intervention.
- Profiling:** the automated analysis of personal data to evaluate specific characteristics or behaviours of an individual.



Australian Privacy Act reforms

What they mean for your organisation.



Consumer survey

We explore consumer attitudes to AI, ADM and customer profiling and find out which industry Australians trust most with their personal info.

We surveyed 1,000 Australian consumers aged 18+ (responses confidential and anonymised).

Read more on [page 7](#)



Brand research

We analysed the AI and ADM management practices of:

- 100 leading Australian brands
- Across 10 industries:

Education and employment
Energy and utilities
Finance
Government
Health and fitness
Information technology
Real estate
Retail
Telecommunications and media
Travel and transport

By reviewing each organisation's public-facing literature, including their website, annual report and privacy policy, we assessed:

- Their commitment to privacy and responsible data handling.
- How they compare to industry best practice.
- How they communicate their policies and practices to customers when collecting their data.

We then aggregated our findings to compare industries, added insights from our consumer survey and used these results to score and rank the 10 industries – this became our 2024 Privacy Index.

Read more on [page 8](#)

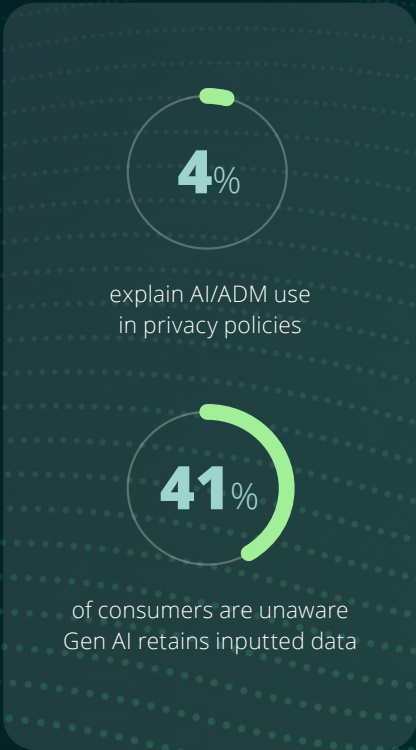


Key findings

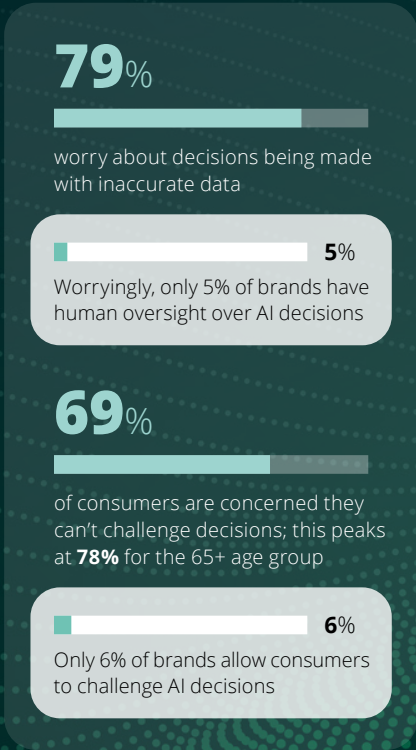
Tech boom: Australian brands love innovative tech



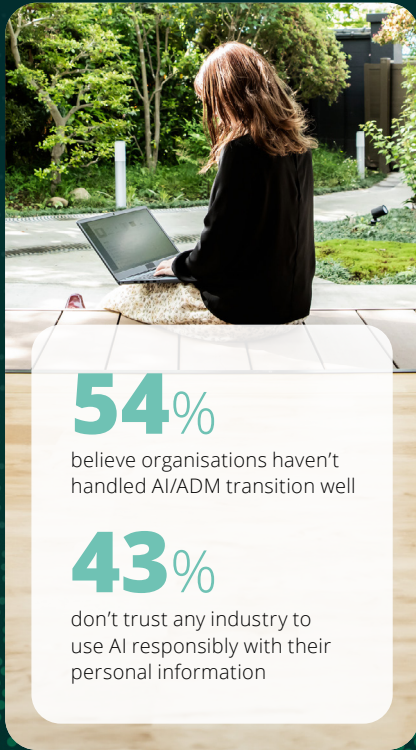
But they don't love sharing its use with their consumers



People are concerned, with good reason



This has led to a privacy trust bust



And trust is hard to rebuild



*Leading Australian brands as selected by our researchers.

Key findings (cont.)

Which is bad for business

- 50% are choosing not to buy a product or service because an organisation asked to collect personal information they weren't comfortable sharing (up from 35% last year)
- 59% limit personal information shared with brands
- 34% changed providers or intend to
- 33% have provided inaccurate information or intend to
- 26% published a negative review or intend to

As a result, people want reforms

88% of consumers believe privacy reforms are crucial

Top 3 reforms consumers most want

-  **Privacy policies:** clear and comprehensive policies that outline how personal information is collected, used, and protected.
-  **Fair and reasonable:** organisations should handle personal information in ways that are fair, reasonable, and not overly intrusive.
-  **Privacy by default:** privacy settings automatically enabled to the highest level of protection for users by default.


Organisations can do more



believe organisations can alleviate concerns by:

- 69% providing clear privacy policies
- 69% positive social media mentions
- 65% not asking for unnecessary information
- 52% focusing on core services over excessive marketing

Doing more leads to trust

 Why is this industry your most trusted?

- I don't hear of data breaches in this field as often and I feel they don't ask for unnecessary information.
- Secure and very few data breaches.
- They have up-to-date technology and cybersecurity measures.
- They have a greater level of honesty and integrity.



Trust is good for business, and Australia!

Privacy Index 2024

How does your industry rank?

When it comes to adopting, implementing and effectively communicating AI and ADM management practices, **how does your industry rank?**

2024 Privacy Index ranking explainer

Top-ranked industries prioritise transparency, accountability and customer empowerment with robust AI and ADM management practices and privacy policies, posing lower risks to consumer data protection.

Bottom-ranked industries are more likely to lack clear communication, customer challenge mechanisms and innovative technology integration, posing higher risks to consumer data protection.

However, some lower-ranked industries may have slower AI adoption rates, which could also contribute to their lower rankings.

It's important to note our assessment is based on publicly available information from privacy policies and annual reports, we don't have detailed insights into if or how organisations use AI/ADM.

2024
ranking

Theme:
AI management*

		2023	2022	2021	2020	2019	2018	2017	2016	2015
1	Education and employment	2	1	4	6	6	9	11	6	N/A
2	Information technology	1	6	1	3	1	1	9	7	7
3	Travel and transport	4	3	3	4	3	5	N/A	8	9
4	Telecommunications and media	6	7	10	8	7	4	3	N/A	10
5	Health and fitness	3	10	7	10	10	8	6	4	4
6	Energy and utilities	5	8	9	7	4	10	4	3	8
7	Real estate	8	4	6	5	2	7	8	13	N/A
8	Retail	9	9	5	1	5	6	7	10	5
9	Finance	10	2	8	9	9	2	1	1	2
10	Government	7	5	2	2	8	3	2	2	1

*The Privacy Index explores a different aspect of privacy each year. It's not for direct year-to-year comparison but offers a comprehensive view of how each industry handles different privacy issues over time.

Consumer Index 2024

Consumer trust takes a nosedive

Who do consumers trust most to handle their personal information?

We asked 1,000 Australian consumers which industry they trust most with their personal information.

Most trusted industry?

Our top answer this year was **‘None of the above’** with **30%**. This paradoxical outcome indicates people’s lack of confidence in any industry to manage their personal information, underscoring the need for all industries to improve their data protection measures and transparency to build public trust.

Government came a close second with **28%** and bottom of the table were real estate and telecommunications and media.



Which industry do you trust most to handle your personal information?

1	None of the above	30%
2	Government	28%
3	Education and employment	12%
4	Finance	12%
5	Health and fitness	7%
6	Information technology	3%
7	Travel and transport	3%
=8	Energy and utilities	2%
=8	Retail	2%
=10	Telecommunications and media	0.5%
=10	Real estate	0.5%

What’s behind the lack of trust?

We asked respondents to explain their choices. Among the 30% who selected ‘None of the above’, for ‘most trusted’ industry, many expressed a general distrust across all sectors, but key concerns included data security, privacy, data collection and transparency.

Comments include:

Breaches in all the above industries is why trust is broken.



At this time, I don’t think any of their systems are as safe as they could be; scammers seem to find a way in.

None of them have put enough effort in to ensure the safe storage of our data, and breaches prove this.

Consumer Index 2024 (cont.)

Government second most trusted industry

Government ranks second on our most trusted list at 28%. This trust is driven by perceived accountability and societal responsibility. One respondent noted, “They have to for the country, or they won’t be re-elected.”

Other reasons include:



Robust security measures and resources: “They have funding and the latest technology.”



Strict legal regulations: “They have rigid privacy laws for retaining the public’s personal information such as tax file numbers.”



Lack of commercial interests: “They have no financial gain by disclosing our information”.

Least trusted industry: telecommunications and media

In a separate question, respondents identified telecommunications and media as the least trusted industry for handling personal information. Major concerns included frequent breaches and lack of transparency in data collection and use.

Comments include:

I’ve already had my personal details compromised.

They have not demonstrated a culture of trust.

They collect a lot of data and share indiscriminately with partners and advertisers.

Our findings reveal significant distrust in organisations’ ability to safeguard personal information and a perception of indifference from many industries.

This distrust is impacting consumer interactions and serves as a stark reminder that reputational damage can be long-lasting.

Investing in robust privacy practices isn’t just a compliance requirement but a strategic necessity to rebuild and maintain consumer trust.



Which industry do you trust least to handle your personal information?

1	Telecommunications and media	26%
2	Government	20%
3	Retail	15%
4	Information technology	10%
5	Real estate	8%
6	Finance	6%
7	None of the above	5%
8	Energy and utilities	4%
9	Health and fitness	3%
=10	Education and employment	2%
=10	Travel and transport	2%

No regrets moves



When adopting AI and ADM technologies, it’s crucial to balance innovation with ethics by consistently asking, “just because we can, should we?” This approach ensures these technologies benefit all parties while maintaining ethical standards.

These ‘no regrets’ moves help organisations develop a responsible framework for AI and ADM adoption, safeguarding privacy and building trust.



Implement ethics-by-design

How?
Integrate ethical considerations at all stages of AI and ADM development and regularly assess ethical boundaries.

Benefit
Aligns technology use with societal values and minimises unethical practices.



Protect personal information

How?
Establish robust policies for protecting and handling personal information.

Benefit
Minimises data breach risks, enhances trust.



Adopt privacy and security-by-design

How?
Design systems with inherent privacy and security features.

Benefit
Safeguards data integrity and confidentiality.



Ensure transparency and consent

How?
Maintain transparency, obtain user consent and disclose AI impacts proactively.

Benefit
Enhances user autonomy and builds consumer trust through clear communication.



Foster a culture of continuous learning

How?
Promote ongoing education with employees about privacy, ethics, and responsible AI use.

Benefit
Cultivates a knowledgeable, ethically aware workforce.



Enhance data clarity and visibility

How?
Map personal information ecosystem to understand what is collected and created, monitor data lifecycle, and manage risks.

Benefit
Ensures responsible use of personal information.



Uplift data protection, quality and security

How?
Embed security measures, validate training data, and minimise data exposure.

Benefit
Reduces risk of breaches, legal challenges, and biases, supports ethical AI outcomes.



Strengthen data governance

How?
Establish clear governance structures and promote awareness.

Benefit
Enables ethical and secure AI strategy and operations.



Chapter 1

The privacy pitfall: The innovation race leaving customers behind

The days of heading to the local bank to discuss a new home loan are mostly gone. Today, with technology and automation playing larger roles in decision-making processes, it's increasingly an AI or ADM algorithm, not a bank manager, deciding our financial fate.





Scored and stored: our data lives

AI and ADM are embedded in daily activities like banking, job applications, navigation, streaming, dating apps, visa applications, online shopping, and holidays. Whatever we're doing and wherever we're going, organisations collect, store, and use our data to create detailed profiles, drawing insights and making rapid decisions about us – the sum of our lives turned into data points, then scored and scaled for eligibility.

Algorithms in action: who's really in control?

It's great for efficiency, but we've lost sight of the decision makers, and a lack of human interaction is creating a disconnect, adding to growing distrust. 'They' know everything about us – dating apps know our 'type', online credit profiles capture every loan pushback, social media remembers every photo and comment – but what do we know about them? Is the algorithm ethical, unbiased, transparent? Is our data properly protected and how is it being used and by whom?

Our digital footprints have wandered beyond our horizon and finding answers can be like chasing shadows.

It's time to shine a light into the darkness.

Tech boom to trust bust

While AI and ADM have been around for years, recent advances in Gen AI have brought them into focus, adding a new level of scrutiny on intelligent automation use, privacy, and responsible data handling. Is this scrutiny justified, or more perception than reality?

Our research shows that **72%** of Australia's leading brands* mention using AI, ADM, or other innovative technologies in their latest annual report, showing a large uptake across the board. However, only **4%** of companies explain in their privacy policy which decisions affecting consumers are made using AI or ADM.

Risk alert! Change is imminent. The first tranche of Privacy Act Reforms requires organisations to disclose in their privacy policies whether personal information will be processed through automated decisions (read more in [Chapter 2](#)).

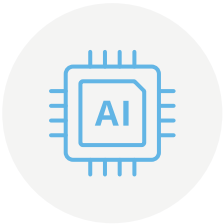
The trust deficit widens

Data breaches and security failures over the years have led to mistrust in institutions' ability to keep people's personal information secure, this lack of transparency around innovative tech further widens this trust gap.

Our consumer survey backs this up with **41%** unaware that Gen AI may retain a copy of inputted data to train future outputs and **54%** saying organisations haven't handled the shift to AI and ADM well. **43%** say they **wouldn't trust any industry** to use automated processes or AI responsibly with their personal information.



*Our findings and statistics apply specifically to these brands chosen by our research team as 'leading'.



Gen AI versus the generations

Our survey reveals that **42%** of respondents use Gen AI, primarily for quick information searches, but use varies significantly across generations, from a low of **17%** in the 65+ bracket, to a high of **74%** among 18-24-year-olds – Gen Zs are clearly storming ahead in AI uptake.

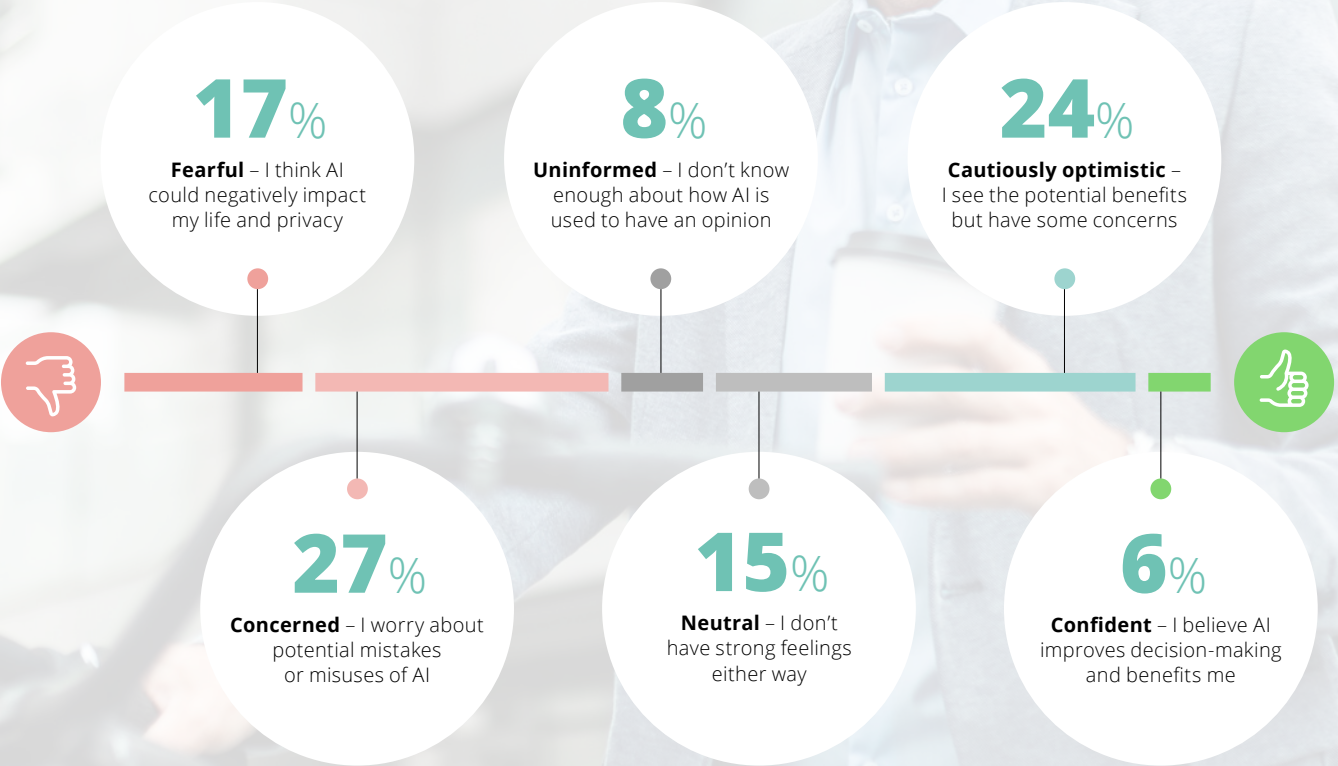
Many people remain cautious though, with only **6%** feeling confident and **24%** cautiously optimistic about AI-made decisions, the remaining respondents have either negative or more indifferent emotions: **27%** concerned, **17%** fearful, **15%** neutral, **8%** uninformed.

These stats reveal the tension between people’s eagerness to experiment with this technology and their apprehension about its implications.

***Tip:** Organisations can help alleviate fears and build trust with openness and transparency. Fit-for-purpose and easy-to-understand notice and consent mechanisms, supported by consumer education and awareness of an organisation’s AI journey are ways to shift the trust dial.*



How do you feel about organisations using AI to make decisions that impact you?



Lack of human connection creates ADM concerns

When it comes to ADM, **68%** of respondents had concerns about its use in society, indicating widespread apprehension. **79%** of those were concerned about automated decisions being made using inaccurate, out-of-date, or incomplete information and **69%** about the inability to challenge decisions. Concern increases with age, peaking at **78%** for the 65+ group.

Consumer concerns:

- I am a person who can't be reduced to data points. I have skills that don't always translate into data.
- I'm concerned bias is fed into the AI that makes the decisions.
- I'm worried decisions are made using incomplete data, and systems are not genuinely intelligent, but purely statistical – a predictor of the most likely, but not necessarily correct outcome.

Aussies are in the dark and powerless

Being unable to challenge AI-made decisions is a concern for most respondents (**69%**). This concern is justified as our research shows only **6%** of companies that disclose the use of AI/ADM say they provide consumers with a right to challenge or opt out of automated decisions. Worryingly, only **5% of companies say they have human oversight** over AI- and ADM-made decisions that affect consumers. While this doesn't necessarily mean there's no oversight or challenge mechanisms as it could be the information isn't being communicated to consumers, it does highlight the need for better oversight, consumer rights, and improved communication.

Risk alert! The government has agreed in principle to a right to object and may proceed in the next tranche of reforms.

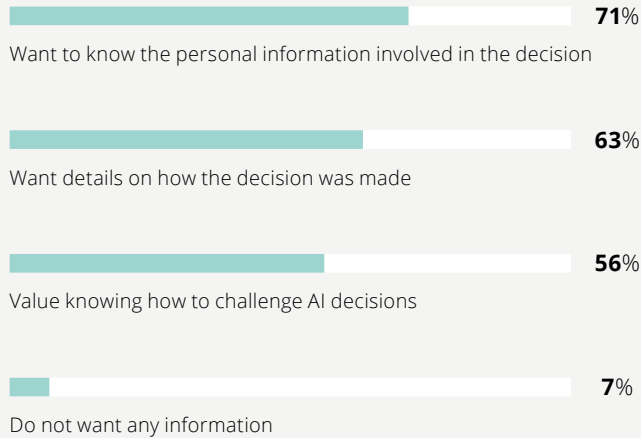
More to me than meets the (data) eye

People want transparency when AI is used to make decisions about them, in particular ones with a significant impact on their livelihood and financial standing, such as job applications, loan eligibility, insurance premiums, visa applications and rental candidacies.

5% Only 5% of companies say they have human oversight over AI or automated decisions affecting consumers.

What consumers want

Consumers demand transparency regarding how AI makes decisions about them.



Lack of trust is bad for business

This lack of trust and transparency, plus feelings of powerlessness are having a tangible impact on consumer behaviour and whether people provide personal information or withhold it.

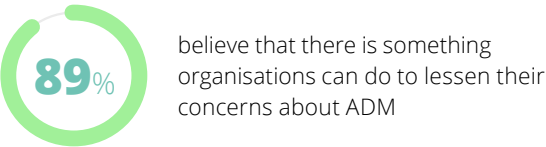
Our survey shows **59%** of respondents have, or will, limit the personal information they give brands.

Risk alert! This behaviour may impact service delivery and data capture, quality, and accuracy, leading to organisational challenges around strategic decision-making, personalisation, effective marketing and maintaining regulatory compliance.

We've seen a significant rise **(50%, up from 35% in 2023)** in the number of respondents choosing not to buy or engage with a product or service to minimise personal information they weren't comfortable sharing.

- 50% are choosing not to buy a product or service because an organisation asked to collect personal information they weren't comfortable sharing (up from 35% last year)
- 34% changed providers or intend to
- 33% have provided incorrect or inaccurate information or intend to
- 26% published a negative review or intend to

It's not too late to win back trust.



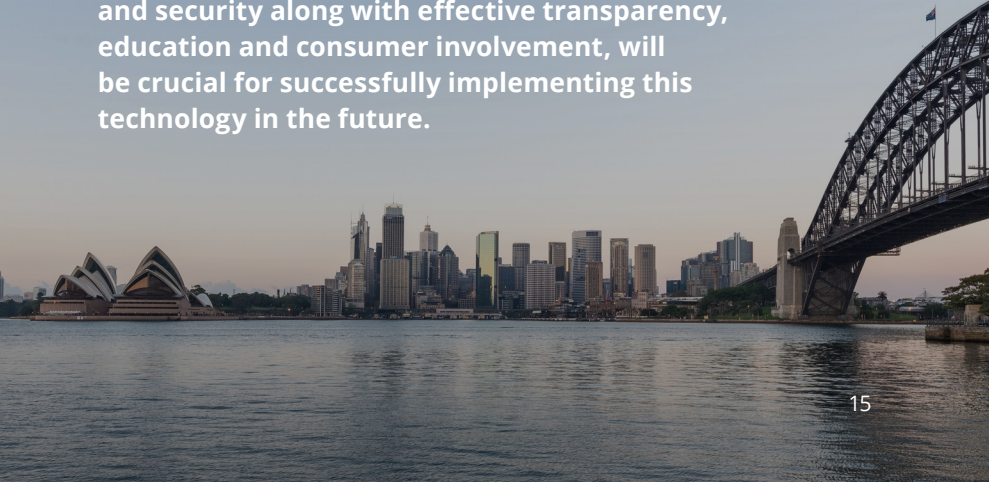
The good news is that 89% of people believe organisations can do more to alleviate concerns by demonstrating they care about privacy. How?



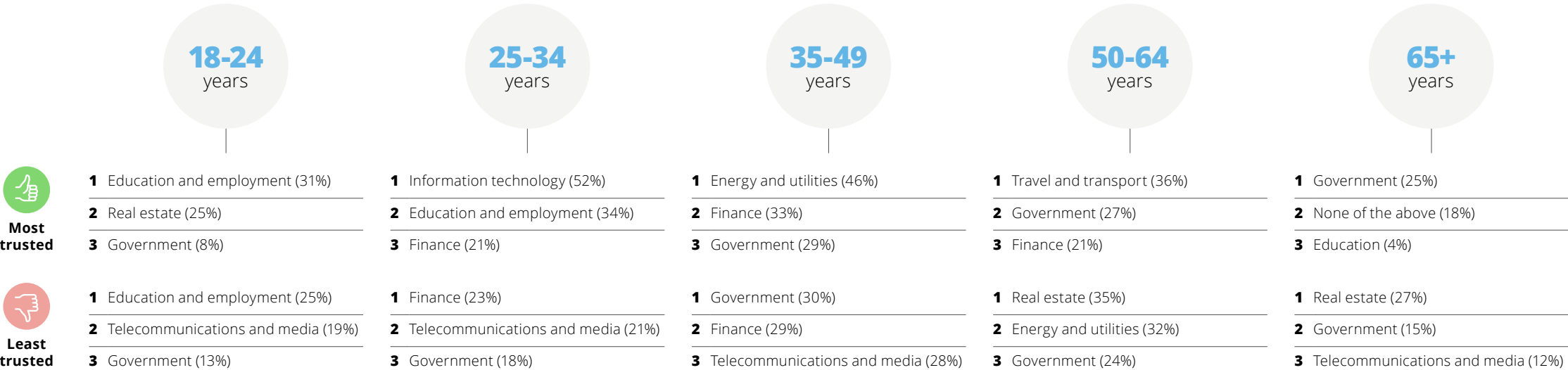
In an era of intelligent automation, the erosion of trust between consumers and brands is a critical issue impacting business success. Transparency and responsible handling of personal information are paramount.

By addressing these concerns proactively, organisations can rebuild trust, improve consumer relationships, and achieve long-term success.

Balancing the use of innovative technologies with adequate controls to support data privacy and security along with effective transparency, education and consumer involvement, will be crucial for successfully implementing this technology in the future.



Which industries are most and least trusted by the generations with their personal information?



Interesting insights



Contrasting views within the generations
As our results come from two separate survey questions, it's possible for an industry to appear in both the top and bottom of the trust rankings. Contrasting views within generations suggest trust in data handling can vary widely even within the same demographic.



Education and employment
While one portion of 18-24-year-olds surveyed rank education and employment as their most trusted, another portion ranks it as least trusted. This highlights the diverse perspectives and experiences within this age group.



Government
Government consistently appears on both the most trusted and least trusted lists across multiple age groups, highlighting significant polarisation in trust towards governmental institutions.



None of the above
A portion of the 65+ age group (18%) trust none of the listed industries to handle their personal information, indicating broad scepticism towards all industries.



Real estate
This sector is consistently one of the least trusted across multiple age groups, particularly among the 50-64 and 65+ demographics, suggesting a need for better transparency and privacy practices.

Chapter 2

Upgrade required: Getting with the (privacy) program

In 1988, Australians lived offline. Banking, shopping, and job applications all happened in real life, and people's personal information was filed in cabinets across the country. 1988 was also the year the country's first privacy legislation was introduced.

IRL to URL: shifting lifestyles

Our lifestyles and how we manage day-to-day affairs has shifted drastically over the last few decades, but has the Privacy Act (1988) evolved to keep up with the challenges of the 21st century?

Today, our personal information is digitised and scattered across cloud databases worldwide. Work and home, social media platforms, government records, e-commerce sites, and smart devices – our data exists in many forms and locations often beyond our reach. The widespread circulation of personal information raises serious and valid concerns about privacy, security, and our ability to control how our information is used.

Preserving and upholding privacy into the digital age

Growing concern around the loss of control of personal information, increased data breaches, as well as lack of transparency and mismanagement of personal information has led to much-needed Australian privacy law reforms.

The reforms aim to give Australians more control over their personal information, organisations more clarity on data protection and increased accountability, and stronger enforcement options for the Office of the Australian Information Officer (OAIC), Australia’s privacy regulator.

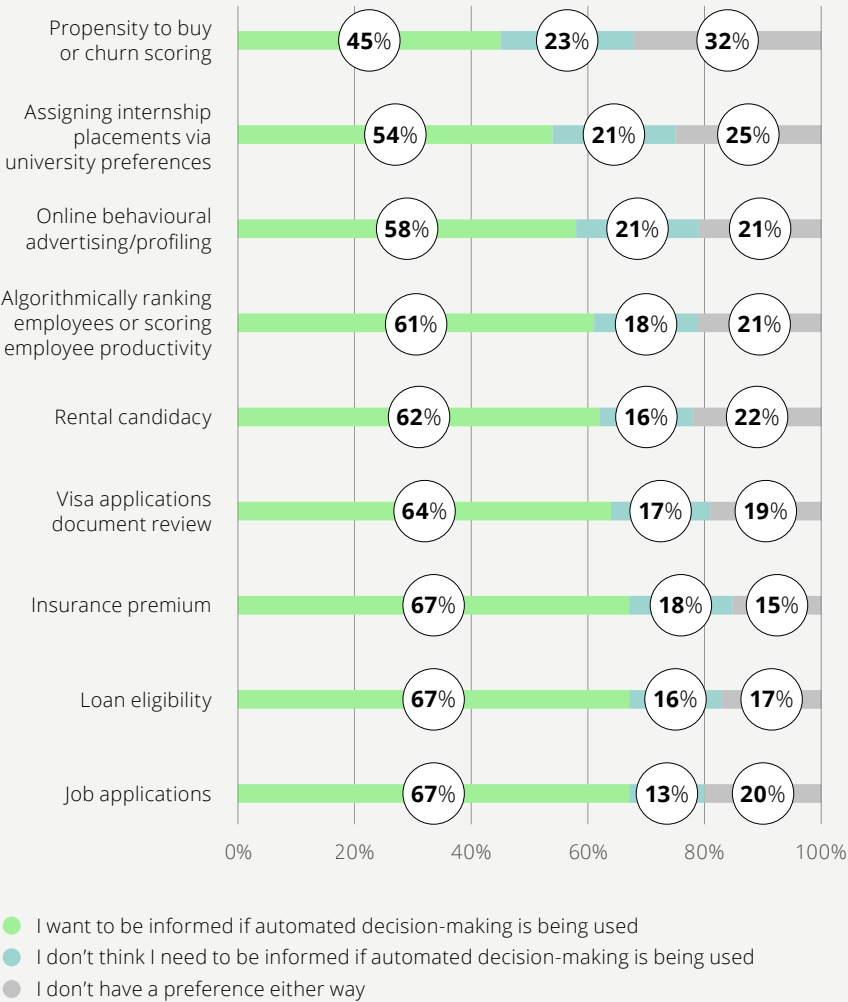
88%

Our survey shows an overwhelming 88% of respondents believe privacy reforms are crucial.

Top 3 reforms consumers most want

- Privacy policies:** clear and comprehensive policies outlining how personal information is collected, used, and protected.
- Fair and reasonable:** organisations should handle personal information in ways that are fair, reasonable, and not overly intrusive.
- Privacy by default:** implementing privacy settings automatically enabled to the highest level of protection for users by default.

When is it most important to know if a company is using automated decision-making tools?





Privacy Act Bill: the reforms and your organisation

Initially, 116 reforms were proposed, with the first tranche of draft legislation – the Privacy and Other Legislation Amendment Bill 2024 (the Bill) – consisting of 23 proposals tabled in parliament on 12 September 2024.

Many substantive reforms aren’t included in this first tranche; however, consumer and public expectations have surged, creating both regulatory and reputational risks for organisations. As technology advances faster than regulations, proactively managing these issues allows organisations to stay ahead of reforms and gain a competitive edge.

Will the reforms adequately protect Australians in the era of intelligent automation? Whether they do or not, what’s evident is consumers want change, and this is the perfect opportunity for organisations to get ahead.

Key AI/ADM-related proposals in the Bill

1. Automated decision making

Reform summary: privacy policies must detail personal information used in significant automated decisions.

Actions for organisations: update privacy policies to include ADM disclosures. Note: If passed, organisations have a transitional period of two years to comply.

2. Children’s Online Privacy Code (COP Code)

Reform summary: the Information Commissioner will develop and enforce a COP Code that aligns with international standards to protect children’s online privacy.

Actions for organisations: implement processes, procedures, and technology to enhance data governance and protection for children’s information.

3. Clarification of ‘reasonable steps’

Reform summary: clarifies that “reasonable steps” in APP 11 include both technical and organisational measures, such as data encryption and staff training.

Actions for organisations: secure information through governance, processes, procedures, and technologies.

4. Penalties and enforcement

Reform summary: introduces new civil penalty provisions, expands the powers of the Court in civil penalty proceedings, and allows the Information Commissioner to issue infringement notices.

Actions for organisations: ensure compliance with APPs and prepare for potential penalties and enforcement actions.

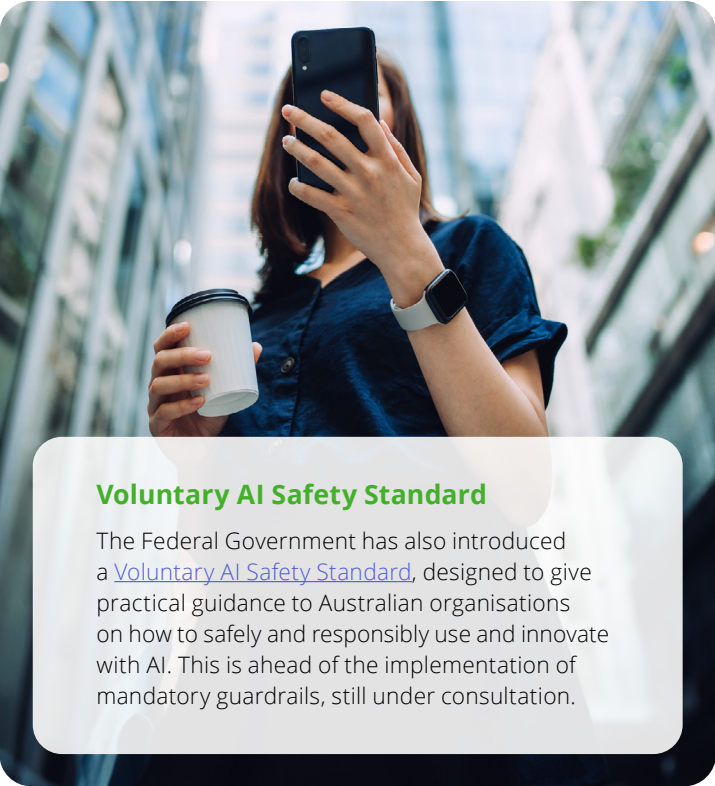
5. Statutory tort

Reform summary: introduces a statutory tort for serious invasions of privacy, allowing individuals to take legal action against privacy invasions.

Actions for organisations: use this as an incentive to enhance existing privacy practices!

Additional reforms

Other reforms include the criminalisation of doxing, eligible data breach declaration, cross-border data flow, ability for the Minister to direct the development of APP codes, emergency declarations, public inquiries, and more robust investigation powers for the OAIC.



Voluntary AI Safety Standard

The Federal Government has also introduced a [Voluntary AI Safety Standard](#), designed to give practical guidance to Australian organisations on how to safely and responsibly use and innovate with AI. This is ahead of the implementation of mandatory guardrails, still under consultation.

Chapter 3

Privacy bootcamp: It's time for a glow-up

Australian privacy reforms and AI standards aren't set in stone yet, but they're on the horizon and our research indicates people want transparency. In an era where AI and ADM are becoming increasingly prevalent, organisations must strike a delicate balance between trust and transparency while ensuring privacy is preserved. By being open about your AI practices, you can alleviate concerns, foster consumer trust, strengthen your cybersecurity posture and position your business as a leader in ethical AI implementation.

Boost your privacy practices and your business

Get ahead with these privacy and data management measures to ensure your business thrives in the digital age.



Enhance clarity and visibility

Do you truly understand how personal information is collected, created, used, combined, and shared within your organisation?

Organisations face an ever-changing ecosystem of personal information, which is often created, combined and processed across multiple systems. Complete clarity and visibility over how personal information flows through your systems empowers your organisation to stay resilient against privacy challenges and ensures responsible use of personal information.

Actions

- 1 Map your personal information ecosystem:** create a comprehensive view of where personal information originates and how it's used.
- 2 Monitor the personal information lifecycle:** as you derive insights from personal information, track and document the processes that generate new personal information.
- 3 Assess and manage risks:** proactively identify and manage personal information and data risks.



Build trust through transparency

Are you being upfront about AI's potential impact with your consumers?

When AI or ADM shapes consumer experiences, transparency is essential. It's not just disclosing when AI is being used – it's being clear, visible, and proactive in showing consumers how these technologies impact them.

Actions

- 1 Make AI visible:** make sure consumers easily understand when AI is influencing their interactions.
- 2 Disclose impacts:** clearly publicise the responsible use of data from outputs to processes.
- 3 Inform proactively:** make sure your policies and portals are easily accessible and clearly explain how consumer data is used.
- 4 Collaborative approach:** Your Chief Data Officer (CDO), Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) should work together to regularly update privacy policies and provide transparency around data use.



Uplift data protection and security

Is data protection and security baked into your AI from day one?

AI and ADM can unlock powerful insights but risk exposing sensitive information without robust security. Neglecting data security, privacy, and ethics at all stages of development and implementation can lead to breaches, legal challenges, and reputational damage.

Actions

- 1 Security, privacy, and ethics by design:** embed robust security measures, privacy safeguards and ethical considerations from the planning and development phase.
- 2 Prevent and respond:** assess your organisation's threat detection capabilities and ensure your incident response plan includes your AI and ADM systems.
- 3 Minimise data exposure:** champion data minimisation and critically assess the necessity of each piece of personal information, including opinions generated about individuals.
- 4 Share your security measures:** demonstrate to consumers that security and privacy are top priorities.



Strengthen data governance

Is your data governance framework equipped to manage the evolving privacy, data and cyber risks of AI and ADM?

AI can't function responsibly without a robust data governance structure. A well-structured governance framework and operating model is crucial for ethical, secure and aligned AI operations. It helps confidently manage risks, enhance compliance and maintain accountability. Establishing clear data governance groups can guide data strategy through management frameworks, policies, and procedures. It also raises awareness of responsible data use through training and education.

Actions

- 1 Establish clear structures:** ensure a key stakeholder in your data governance function actively oversees AI strategy, management, and compliance.
- 2 Align and empower:** align data governance practices with business objectives so they're adaptable as the organisation grows.
- 3 Promote awareness:** consistently train teams on responsible and trustworthy AI practices and ensure clear C-suite level accountability.



Ensure data integrity

Can you trust the data training your AI systems?

AI and ADM output is only as good as the data they're fed. To avoid biased or inaccurate results, data quality is vital. Clean and de-identified personal information must be non-negotiable. Organisations must adopt a rigorous approach to data integrity as compromised data can lead to misleading insights and significant privacy risks.

Actions

- 1 Assess data quality:** regularly validate your training data to ensure it's accurate, complete, and unbiased.
- 2 Use clean data:** ensure de-identification of personal information and data minimisation is standard practice across your AI systems.
- 3 Ethical AI outcomes:** continuously monitor AI outputs for ethical issues and ensure issues can be escalated and managed so models perform without bias.



Advance A(I)ustralia fair

Savvy organisations need to seize this opportunity to get ahead of legislation and ensure their privacy practices are fair, ethical, secure, and protect their business and consumers into the future.

Investing now in robust AI and ADM management practices helps mitigate risks and build consumer trust to foster loyalty and drive long-term success.

This is your chance to build a competitive advantage, showcase your commitment to privacy and ethical standards and become a trusted leader in an increasingly complex digital landscape.

Contacts

Lead Partners

Daniella Kafouris
Technology & Transformation
dakafouris@deloitte.com.au

Lucy Mannering
Technology & Transformation
lmannering@deloitte.com.au

About the team

The privacy specialists in our Technology & Transformation Practice who developed the Deloitte Australia Privacy Index 2024 included:

Lead Senior Manager

Shan Evans

Project coordinators

Dina Gouda
Lucy Goodin
Alcina Giang

Editorial lead

Kate O'Brien

Project writers

Graham Chikaka
Samantha Santa-Isabel

Design

Vincent Pauletti

Research

Caroline Goromonzi
Joshua Kiriakoff
Catherine Guo
Maria Zotti
Anna Ng
Anushiya Achudhan

Contributors

Amanda Leong
Siddharth Desai
David Alonso
Geena Williment
Nina Yiannopoulos
Tracey Tran



This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.com.

About Deloitte Asia Pacific

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia’s leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 10,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www2.deloitte.com/au/en.html

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2024 Deloitte Touche Tohmatsu

1452870443_Designed and produced by The Agency | Deloitte Australia_11/24