Australian Government
Office of the Australian Information Commissioner

Australian Community Attitudes to Privacy Survey

May 2026

OAIC

OAIC research

The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency in the Attorney-General's portfolio, established under the *Australian Information Commissioner Act 2010 (AIC Act).*

We are responsible for promoting and upholding information access rights under the *Freedom of Information Act 1982 (FOI Act) and upholding the privacy rights of Australians under the Privacy Act 1988* (Privacy Act).

Our research helps to inform our approach to regulation, law reform, strategy and education. OAIC research is available at: oaic.gov.au/research

For enquiries about OAIC research, please contact communications@oaic.gov.au

Acknowledgments

The OAIC acknowledges Traditional Custodians of Country across Australia and recognises their continuing connection to lands, waters and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures, and to Elders past and present.

The OAIC would like to thank the Social Research Centre who conducted this research on our behalf and developed this report.

The project was led by Director, Shane Compton and the project team consisted of Susie Tian and Alison Eglentals.

Copyright

Suggested reference

Office of the Australian Information Commissioner (2026) *Australian Community Attitudes to Privacy Survey 2026,* Office of the Australian Information Commissioner, Australian Government.

Contents

Commissioners' foreword

Australians' expectations about privacy continue to sharpen as the information ecosystem becomes more complex, data-intensive and difficult to navigate. The 2026 Australian Community Attitudes to Privacy Survey (ACAPS) points to a community that places a high value on privacy, but does not consistently experience privacy protections as workable in practice. Trust is uneven across sectors, and wariness of emerging technologies is increasing, particularly in terms of fairness, accountability and the practical ability to exercise rights. Australians want greater transparency, more proportionate collection of personal information, and a fairer go when using digital services.

The right to privacy and the right to access information are protected and promoted by the Office of the Australian Information Commissioner (OAIC). The ACAPS findings go to broader issues beyond privacy such as information access and encompass the full range of the OAIC's regulatory 2025-26 priorities, which include a focus on rebalancing power and information asymmetries, and rights preservation in new and emerging technologies. This survey builds on the cross-jurisdictional 2025 Information Access Study, which showed Australians expect accountability, transparency, and clear access to government information – particularly where technology such as artificial intelligence (AI) is being used to support automated decisions.

Just as technology is proving to be a means to rapidly transmit information its deployment is impacting public trust. This is because data handling is arguably not keeping pace with community expectations, and hampering Australians' engagement in the digital economy. Greater confidence in how personal information is handled would increase Australians' willingness to use digital services or programs that require sharing personal information. Around two-thirds (68%) say they would be more likely to use such digital services if they felt their data was handled fairly and responsibly.

ACAPS shows that while 93% say protecting personal information is important to them and 87% say they are more concerned about privacy than 5 years ago, many do not feel able to act on that concern day-to-day. Consent is often experienced as a gateway: 65% say sharing information rarely or never feels like a genuine choice and 68% say the same about consent. A substantial proportion of the community (78%) report very little or no real control over how their personal information is collected and used, and 52% say they accept sharing because they might otherwise miss out on essential services or opportunities. This points to persistent power and information asymmetries not addressed by notice and consent alone.

Australians also draw clear fairness boundaries. Only 10% say organisations' real-world data practices are usually fair, while 35% say they are mostly or always unfair. Fairness concerns appear to concentrate around disproportionate collection, limited or unrealistic opt-out, and situations where benefits are perceived to flow mainly to organisations. There is strong rejection of practices associated with data brokerage and advertising technology, alongside expectations for stronger limits on collection, retention and secondary uses. Australians feel that when an entity collects their personal information for one reason, it is often not fair or reasonable for them to use it for another reason. For example, 93% say it is not fair and reasonable for an entity to use the personal information they collected to provide a product or service to train AI models. The survey also indicates a strong boundary around using personal information to train AI systems after a service they have received has ended (71% say this is unacceptable), reinforcing the importance of purpose limitation and lifecycle controls.

Expectations are clear for new and emerging technologies. AI is a widely recognised privacy risk (69%), trust in AI companies is low (4%), and acceptance of AI uses involving personal information appears contingent on protections that make high impact uses transparent and contestable. Australians most frequently prioritise a right to human review (81%), limits on how personal information is retained by third-party providers (80%), and being told when AI is being used (79%). This underscores the importance of the forthcoming automated decision-making (ADM) transparency obligation, which will require regulated entities to disclose the use of AI and ADM in their privacy policies from December 2026.

As the government sector expands its use of technology to inform decision making and deliver services, preservation of information access rights is increasingly important.

This emphasis on transparency was mirrored in the 2025 Information Access Study that found a significant majority of Australians (86%) also agree that the government must publicly report on any technology used to inform freedom of information decision-making (including AI and automated decision-making).[1] The OAIC's January 2026 report into ADM highlighting transparency obligations under the FOI Act shows that much needs to be done to ensure Australians are aware of how their information is used by government agencies. As a responsive regulator, the OAIC is focused on strengthening the information governance of the Australian Public Service and ensuring timely access to government information. In providing the ADM Report and guidance to government agencies, the OAIC recognises the efficiency and productivity gains that can be delivered through technology to a community that is confident to engage with digital services and better equipped to exercise related rights, including seeking a review of a government agency decision.

ACAPS highlights the gap between formal rights and lived experience. Two in 5 Australians (40%) say they do not really know what data organisations hold about them or how to access it, and only 11% say they can easily access their data and request corrections or deletion. Even where concerns arise, action is not assured: 64% had concerns in the past year, but 52% did not raise them, often because they felt it would not make a difference (56%), would be too hard or time-consuming (51%), or they did not know how (40%). This reinforces the importance of clear, timely and accessible pathways for access and redress.

Australians demand transparency, both in understanding their privacy rights, how their information is used, and in embracing their right to access that information. Improving transparency will strengthen the community's already active engagement with these systems and safeguard a healthy, informed and vibrant democracy.

Carly Kind	**Elizabeth Tydd**	**Alice Linacre**
Privacy Commissioner	Information Commissioner	FOI Commissioner

1 2025 Cross-jurisdictional Information Access Study Information access survey | OAIC Information access survey highlights strong community engagement

Overview

The 2026 Australian Community Attitudes to Privacy Survey (ACAPS) is a nationally representative tracking study (n=1,504, fieldwork 16–30 March 2026) that monitors Australians' attitudes to privacy, experiences of privacy risks and misuse of personal information, and expectations of organisations and government. ACAPS 2026 also explores issues including perceptions of consent and control, fairness and proportionality in collection and use, complaint and dispute resolution, support for deletion/erasure, and attitudes to artificial intelligence (AI) and biometric uses involving personal information.

The study evidences that privacy remains important to Australians and concern is increasing. Many Australians feel they do not have meaningful control over how their personal information is collected, used and shared in practice. Trust is concentrated in health providers and government, and is very low in digital and data-driven sectors such as social media, AI companies and data brokers. Australians draw clear lines between necessary collection for service delivery, and practices they view as excessive, opaque or one-sided, particularly secondary uses such as targeted advertising based on sensitive data, trading or sale of personal information, and training AI systems. Strong support for deletion rights and for extending privacy obligations to currently exempt sectors points to an expectation that privacy protections should be practical, enforceable and matched to contemporary data practices.

Headline findings

Relevance and accountability

- **Privacy remains a key issue**. 93% say protecting personal information is important to them, and 87% say they are more concerned about their privacy than they were 5 years ago.
- **Australians overwhelmingly expect organisations to minimise privacy risks**. Almost all respondents (98%) say organisations that collect, use or share personal information should be responsible for protecting privacy even if no immediate harm occurs, with 86% viewing this responsibility as very strong.
- **Greater confidence in privacy practices would increase participation in digital services**. Around two-thirds (68%) say they would be more likely to use digital services requiring personal information if they believed their data was handled fairly and responsibly.
- **Australians remain cautious about the use of artificial intelligence (AI) in decision-making that may affect them**. Nearly all (96%) say some conditions should be in place before it is used. Around 7 in 10 Australians (71%) consider it somewhat or very uncomfortable for organisations to use personal information originally provided for a service to train AI systems after that service has been completed. AI use for fraud detection is more widely accepted (64%). Acceptance is lowest for automated eligibility or risk-based decisions, such as loan approvals or benefit eligibility, with only one-quarter (25%) viewing this as acceptable.

Control and consent in practice

- **Most people feel they have limited real control**. 78% report very little or no control over how their personal information is collected and used.
- **Consent often doesn't feel like a genuine choice**. 65% say sharing information rarely or never feels like a genuine choice and 68% say the same about consent. 52% say they accept sharing because they might otherwise miss out on essential services or opportunities.
- **Data collection is accepted when clear limits and choices exist**. Around 9 in 10 Australians (92%) say data collection can be acceptable under certain conditions, particularly where the purpose is clear (69%), consent or opt-in is available (68%), collection is limited to what is necessary (66%), and the ability to opt out of non-essential collection (61%).
- **Privacy policies are expected to do a lot, but are often skipped.** While people know what they want included, 69% say they always or often agree without reading most or all of the policy.

Everyday concerns and impacts

- **Privacy concerns are widespread.** 73% (vs 64% in 2023) experienced a privacy concern in the past 12 months.
- **Marketing-related issues are common.** The most common concerns were being unable to unsubscribe from marketing (41% vs 25% in 2023) and having information used for unsolicited direct marketing (38% vs 21% in 2023).
- **Impacts are felt quickly.** Among those who experienced a concern, 70% (vs 55% in 2023) reported more scams/spam, 46% (vs 53% in 2023) reported loss of trust and 39% reported loss of control.
- **Harms following data breaches remain widespread**. Around three-quarters (77%) of Australians whose data was involved in a breach experienced at least one form of harm, while exposure to scams and spam increased and was the most common impact (62% vs 52% in 2023).

Fairness boundaries, collection limits and trust

- **Many Australians judge current data practices as unfair.** Only 10% say organisations' real-world practices are usually fair, while 35% say they are mostly or always unfair.
- **Secondary uses are a key 'red line'**. Around 9 in 10 say it is not fair and reasonable to use personal information for selling/trading personal information (96% vs 87% in 2023), online tracking, profiling and targeted advertising to children (96% vs 89% in 2023) or other vulnerable individuals (95% vs 88%), unnecessary location tracking (94% vs 87%), training AI models/products (93%), significant AI-informed decision (91% vs 70%), differential pricing (91%), or targeted advertising based on sensitive data (91% vs 84% in 2023). Around 7 in 10 (71%) consider it unacceptable for organisations to use personal information provided for a service to train AI systems after the service has been completed.
- **People distinguish between necessary and excessive collection**. Individuals view the provision of basic identifiers to access a service as reasonable, but 92% say there are some types of information organisations should never collect. Information about sexual orientation (72%) and biometrics (71%) feel excessive or unjustified in most situations, regardless of the organisation or purpose.
- **Trust varies sharply across sectors and has declined across many commercial industries**. Trust remains highest for health service providers (74%) and government agencies (68%), but has fallen across insurance, telecommunications, technology, retail and real estate sectors since 2023. Trust is lowest for social media companies (3% vs 14% in 2023), data brokers (4%) and AI companies (4%).

Rights, redress and support for stronger protections

- **Many people don't feel equipped to use their rights.** 40% do not really know what data organisations hold about them or how to access it, while 11% say they can easily access their data and request corrections or deletion.
- **Concerns often don't become complaints, and pathways appear hard to navigate**. 64% had concerns in the past year, but 52% did not raise them. Among non-complainants, 56% said it would not make a difference, 51% said it would be too hard/time-consuming, and 40% did not know how. Among those who did complain, only 9% said the issue was resolved to their satisfaction.
- **Confidence in privacy complaint handling varies by sector**, with banks and financial institutions (46%), health services (42%) and government agencies (41%) rated highest, and very low confidence in online retailers (4%) and social media platforms (3%).
- **Support for stronger rights and broader coverage is very high.** 93% support a legal right to request deletion of personal information, and there is strong support for extending equivalent privacy obligations to currently exempt sectors.

What the findings mean for the community and for industry

For the community, the results reinforce that privacy risks are experienced as practical, everyday issues in the form of spam and scams, marketing friction, uncertainty about who holds what data, and limited ability to meaningfully opt out. The strong emphasis on control, fairness and accountability suggests Australians expect organisations to implement privacy safeguards that work in the moment decisions are made, not only through long-form policies or complex consent flows. High support for deletion and concern about secondary uses (including AI training) indicates an expectation that organisations should not repurpose personal information indefinitely or in ways that are difficult to see, contest or reverse.

For industry, the findings point to a sustained 'trust gap' for sectors that rely heavily on data-driven business models, particularly where collection feels excessive, benefits appear one-sided, or there is no realistic alternative to participation. The results suggest that building trust is likely to depend on:

- clearly limiting collection and retention to what is reasonably necessary and proportionate
- constraining secondary uses (especially high-impact uses and uses involving sensitive information)
- giving people practical choices that do not require trading away access to essential services in exchange for the secondary use or disclosures of their personal information
- providing complaint, access and correction pathways that are easy to find, easy to access, predictable and effective.

Where AI and biometrics are used, community acceptance appears strongly conditional on transparency, contestability (including human review), and clear boundaries around training, sharing, retention and secondary use.

What the survey tells us about the OAIC's regulatory priorities

1. Making privacy choices fairer and easier to understand

What the survey suggests: Many Australians experience 'consent' as a condition of participation rather than a genuine choice, and fairness concerns rise when collection feels disproportionate or opting-out is unrealistic.

Regulatory implication / opportunity: Set clearer expectations of necessity and proportionality and stronger limits on collection, retention and secondary use beyond notice-and-consent, especially in high-risk and data-intensive business models.

2. Protecting privacy rights as new technologies develop

What the survey suggests: Acceptance of AI and biometrics is strongly conditional: people want transparency, boundaries on secondary uses (including AI training), and the ability to challenge high-impact outcomes.

Regulatory implication / opportunity: Promote guardrails for AI/biometrics in particular purpose limitation, contestability (including human review where appropriate), strong transparency, and lifecycle controls on use, sharing and retention.

3. Improving how government manages information

What the survey suggests: Trust in government agencies' handling of personal information is higher than in 2020 and remains consistent with 2023 levels, but it is conditional on disciplined stewardship, particularly where decisions affect rights and entitlements and where government uses AI.

Regulatory implication / opportunity: Reinforce public sector governance as a benchmark: clear accountability, risk assessment and oversight before high-impact deployments, and transparent practices and disclosures that sustain community trust.

4. Ensuring timely access to information and effective pathways

What the survey suggests: Many people are not confident they can access, correct or delete their personal information, and privacy concerns often do not progress to complaints because pathways feel unclear, burdensome or ineffective.

Regulatory implication / opportunity: Encourage improved accessibility and predictability of complaint pathways (clear contact points (including outside of logged in accounts), reasonable timeframes, and outcomes that build confidence) so rights operate as practical tools and generate system feedback.

Methodology snapshot

ACAPS 2026 surveyed 1,504 adults aged 18+ across Australia (weighted to be nationally representative). Data collection was conducted via the Life in Australia™ probability-based panel, primarily online (n=1,490) with a small proportion by telephone (n=14). Fieldwork ran from 16–30 March 2026.

Introduction to privacy

Australians are increasingly concerned about their privacy and are recognising a broader range of risks, particularly around data security, misuse of personal information, and how data is handled by organisations and digital technologies. While there is strong and growing support for privacy protections, data minimisation, and rights such as access and deletion, many feel they lack understanding, control and genuine choice, with widespread disengagement from privacy policies reinforcing this gap. This points to a clear disconnect between expectations and lived experience, alongside growing demand for greater transparency, accountability and control.

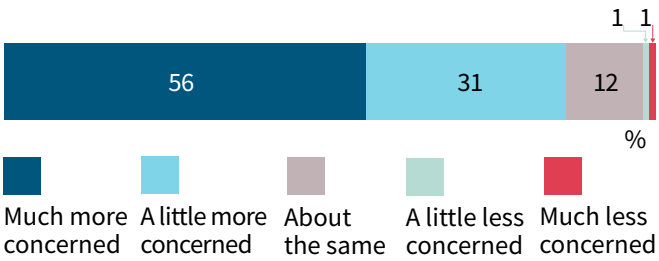
Within this context, privacy remains meaningful in consumer decision-making. Although not the primary driver compared with service quality and price, it consistently ranks ahead of convenience, indicating that many Australians are willing to trade ease or speed for stronger privacy protections. This reflects a broader shift towards more privacy-conscious behaviour, particularly among those with higher levels of concern about how their personal information is handled.

Shift in privacy concern overtime

Compared with 5 years ago, Australians are more concerned about their privacy, with almost 9 in 10 (87%) saying they are a little or much more concerned.

Increased concern about personal privacy is more pronounced among women than men (90% vs 83%).

Figure 1 Concern about privacy compared to 5 years ago



Much more/A little more concerned **87**

Bar chart segments follow the same left-to-right order as the legend

G14. Compared with 5 years ago, how concerned are you about your privacy now?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (<0.5%) and refused (0%) not displayed.

Perceived privacy risks

Overall, Australians identify a broader range of privacy risks in 2026 than in 2023, with increases observed across all measures of perceived privacy risk presented in the survey. This suggests privacy concerns are becoming more common and broader, going beyond single incidents to include wider concerns about how personal information is collected, used and managed. Data security failures and misuse of personal information remain the most commonly mentioned risks, with concern focused on organisational practices as well as external threats such as scams. There is also broader unease about how personal information is collected, shared and used across digital platforms and emerging technologies, including AI.

The biggest privacy risks identified by Australians include:

- data breaches (82%, up from 74% in 2023)
- organisations not storing personal information securely (77%, up from 60% in 2023)
- scammers attempting to access personal information (75%, up from 71% in 2023)
- organisations sending information overseas (70%, up from 50% in 2023)
- concern about AI systems using personal information (69%, up from 43% in 2023).

Together, these findings suggest that perceived privacy risks are linked to weaknesses in organisational systems, poor information handling and security by organisations, and harmful actions by outside parties.

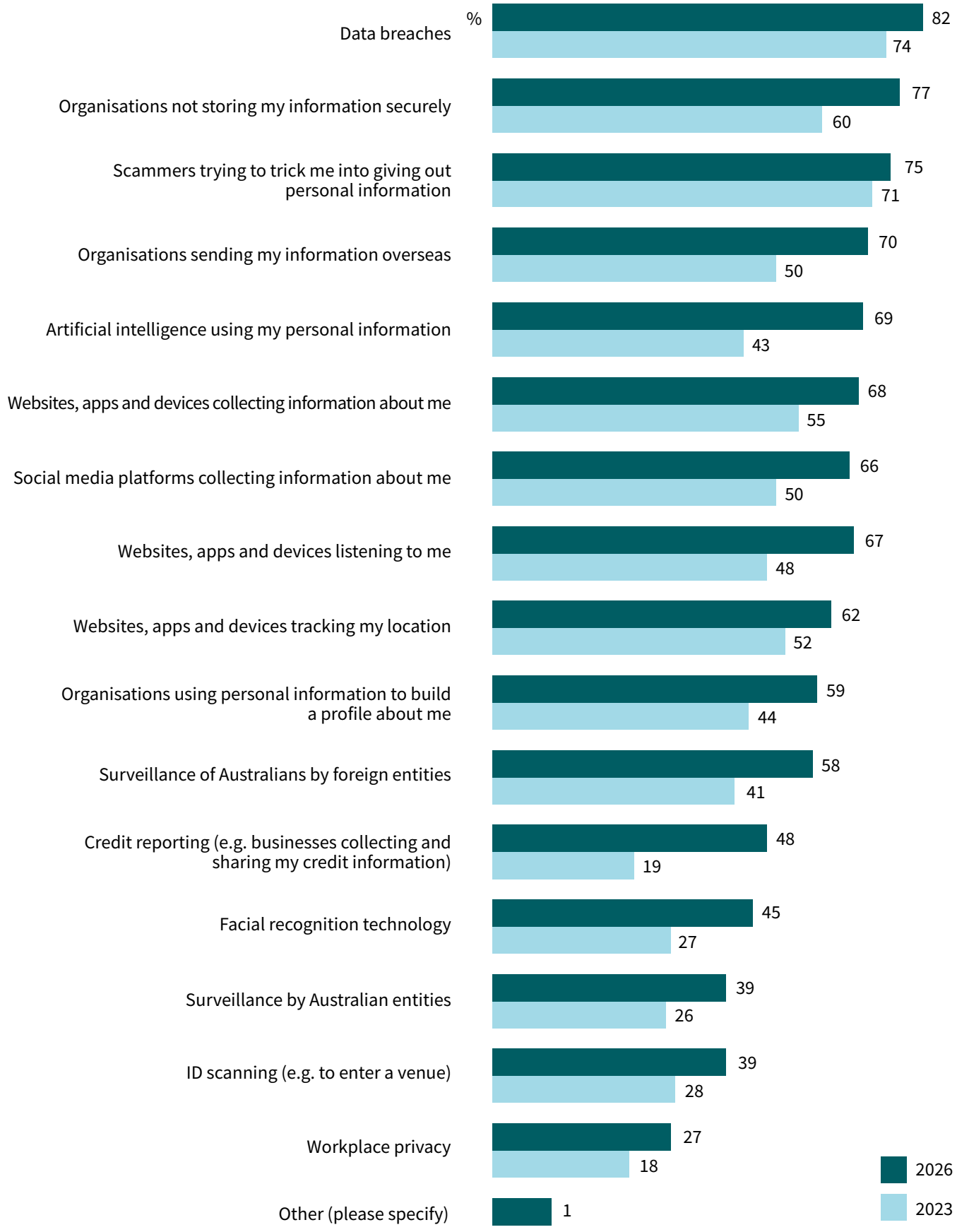
Australians with higher overall privacy concern tend to identify a wider set of privacy risks. This group is more likely to include people who:

- have previously had concerns about how organisations handle their personal information
- feel they have little or no control over how their information is collected and used
- report rarely or never having a choice about sharing personal information.

Awareness of recent data breaches in Australia is associated with higher concern about data breaches, regardless of whether individuals were personally affected, suggesting that public visibility of incidents may shape perceptions of risk.

Concern about organisations not storing information securely is more pronounced among Australians aged 50+ (86% vs 70% of those aged 18–49) and among English-only speakers (81% vs 67% of those who speak a language other than English at home), indicating variation in how privacy risks are perceived across population groups.

Figure 2 Perceived privacy risks



Bar chart segments follow the same top-to-bottom order as the legend

P1. What do you think are the biggest privacy risks that you face today?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,626)
Notes: Don't know (1%) and refused (<0.5%) not displayed. "Credit reporting" label was updated to "Credit reporting (e.g. businesses collecting and sharing my credit information)" in 2026, so comparisons with 2023 should be interpreted with caution.

Beliefs about protecting personal information and expectations for organisations to act fairly

Australians place a very high value on data privacy and express strong expectations for greater control over how their personal information is handled. Almost 9 in 10 agree or strongly agree that:

- protecting their personal information is important (93%, up from 62% in 2023). *Comparison with 2023 should be interpreted with caution due to changes in question wording (2023 wording: "Protecting my personal information is a major concern in my life")*
- they want more control and choice over how their data is collected and used (87%, up from 84% in 2023).

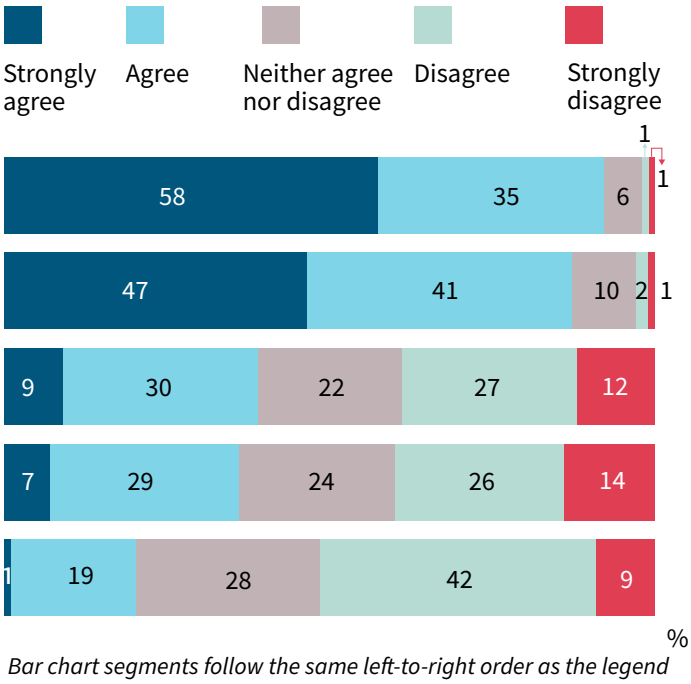
At the same time, perceptions of control appear more limited, suggesting a gap between expectations and lived experience. Individual responsibility and agency for protecting privacy is becoming more complex, with individuals appearing increasingly fatalistic about their privacy as shown by the following.

- A growing share of Australians agree that protecting their privacy is too much effort (39% vs 28% in 2023).
- Fewer Australians report feeling in control of their data privacy, with only 1 in 5 (20%) agreeing that they are in control, down from 32% in 2023.

Taken together, these patterns suggest increasing concern about privacy alongside declining confidence in individuals' ability to manage their personal information.

Perceptions that protecting personal information requires too much effort are more commonly reported among Australians aged 18–34 (48% vs 33% of those aged 50+), people living in capital cities (42% vs 33% outside capital cities), those with tertiary education (47% vs 34% with vocational qualifications), and those who speak a language other than English at home (51% vs 35% of English-only speakers).

Figure 3 Beliefs around control over personal information



Bar chart segments follow the same left-to-right order as the legend

	Strongly agree/agree		
	2020	2023	2026
Protecting my personal information is important to me*	70	62	93
I want more control and choice over the collection and use of my personal information	87	84	87
It is too much effort to protect the privacy of my data	30	28	39
None of our personal information is private anymore, we need to get used to it	38	35	36
I feel I am in control of my data privacy	34	32	20

G5. Thinking about data privacy, to what extent do you agree or disagree with the following?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,916, 2020: n=1,505)
Notes: Don't know (0%) and refused (0%) not displayed.
* Comparison with 2023 should be interpreted with caution due to changes in question wording (2023 wording: "Protecting my personal information is a major concern in my life")

Australians strongly believe that organisations which collect or hold their personal information should be responsible for protecting it. This includes using privacy-protective default settings and limiting how much information they collect.

Around 9 in 10 Australians agree or strongly agree that:

- privacy settings should be most protective by default (93%)
- they would choose to share only minimal personal information (88%).

At the same time, many feel uncertain and constrained, with 3 in 5 agreeing they do not understand how organisations use their data (61%), and they have no choice but to accept data practices to access services (58%, up from 50% in 2023).

Attitudes towards accepting privacy trade-offs for convenience or personalisation are mixed, with less than half agreeing or strongly agreeing that:

- they would prefer targeted ads if they must receive ads (47%, down from 53% in 2023)
- it is fair to share some data to use services (47%%, down from 55% in 2023).

Perceived control and transparency remain low, with only about a quarter agreeing or strongly agreeing that:

- they can control how most services use their data through settings (24%, down from 39% in 2023)
- most organisations are transparent about how personal information is used (24%, down from 42% in 2023).

This highlights a clear gap between Australians expectations for privacy and perceptions of current practices by organisations entrusted with their personal information.

Australians are more likely to think it is fair to share personal information to use a service when they also feel they have choice and control over how their information is handled. This includes those who:

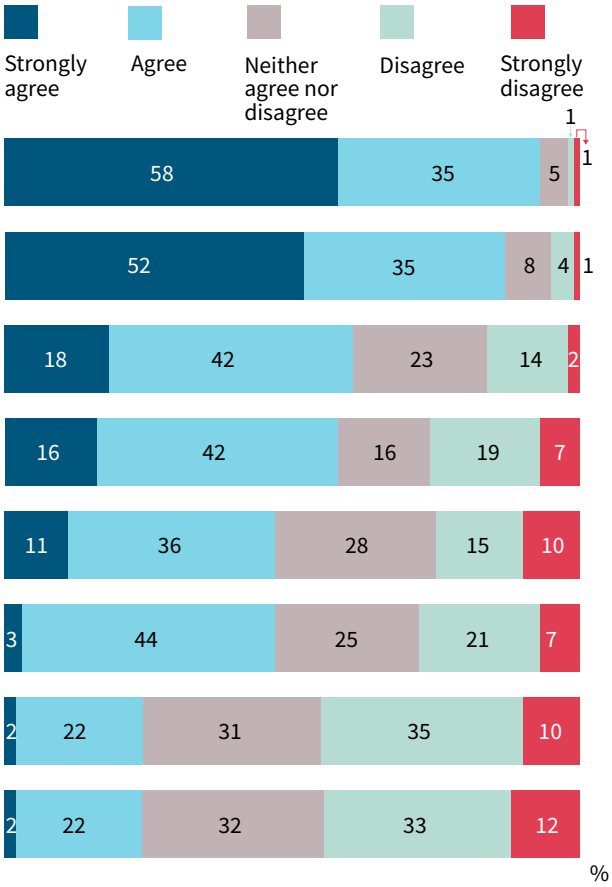
- feel they have some or a great deal of control over how their personal information is collected and used (57% vs 44% of those feel very little or no real control)
- feel that sharing personal information is always, often or sometimes a real choice in everyday situations (53% vs 44% of those feel rarely or never a choice).

Older Australians aged 50+ (56% vs 40% of those aged 18–49) and those living outside capital cities (51% vs 45% of those in capital cities) are more likely to prefer targeted and relevant advertising.

Limited understanding of how organisations use personal information is also higher among those aged 25–34 (65%) and 65+ (67%), compared to 49% of those aged 18–24 and 55% of those aged 50–64.

Perceived transparency in how organisations handle personal information is higher among older Australians aged 65+ (36% vs 21% of those aged 18–64) and those without formal qualifications (33% vs 24% average Australian).

Figure 4 Beliefs about organisations' personal information handling practices



	Strongly agree/agree		
	2020	2023	2026
Privacy settings should be the most privacy protective by default	N/A	N/A	93
If I could choose to hand over only minimal personal information, I would	N/A	N/A	88
I don't understand what organisations do with the information they collect about me	58	58	61
If I want to use a service, I have no choice but to accept what the service does with my data	46	50	58
If I must receive ads, I'd prefer them to be targeted and relevant to me	48	53	47
It is fair enough that I share some personal information if I want to use a service	58	55	47
Most services I use allow me to control what the service does with my data, and I know how to use the settings	N/A	39	24
Most of the organisations I deal with are transparent about the way they use my personal information	N/A	42	24

Bar chart segments follow the same left-to-right order as the legend

G6. Thinking about data privacy, do you agree or disagree with the following?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,916, 2020: n=1,505)
Notes: Don't know (0%) and refused (0%) not displayed.

Engagement with privacy policies

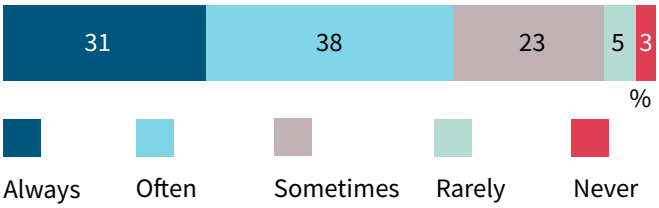
Around 7 in 10 Australians (69%) report that they always or often agree to a company's privacy policy without reading most or all of it in the past 12 months, particularly those aged 18–64 (72% vs 58% of those aged 65+) and those living in capital cities (71% vs 64% outside capital cities).

Those who always or often accept privacy policies without reading them are just as likely as the average Australian to say they are more concerned about privacy than they were 5 years ago (87%). This suggests that routinely accepting privacy policies without reading them may not necessarily reflect low concern about privacy, but could instead be associated with feelings of limited choice or control. Compared with those who read privacy policies at least sometimes, this group is more likely to:

- report limited understanding of how organisations use their personal information (63% vs 56%)
- feel that consent (73% vs 56%) or sharing personal information (72% vs 51%) is rarely or never a real choice
- feel they have little or no control over how their data is collected and used (82% vs 69%)
- accept sharing personal information because not sharing them would mean missing out on essential services or opportunities (57% vs 40%)
- agree that privacy settings should be most protective by default (95% vs 89%)
- prefer minimal data collection (90% vs 82%).

Taken together, these findings indicate people feel reading privacy policies does not meaningfully change outcomes, particularly when services are seen as essential or opting out is difficult. This aligns with broader concerns about whether current data practices provide Australians with meaningful choice and control, and with expectations for stronger organisational privacy protections.

Figure 5 Agreeing to a company's privacy policy without reading it in the past 12 months



Always/Often **69**

Bar chart segments follow the same left-to-right order as the legend

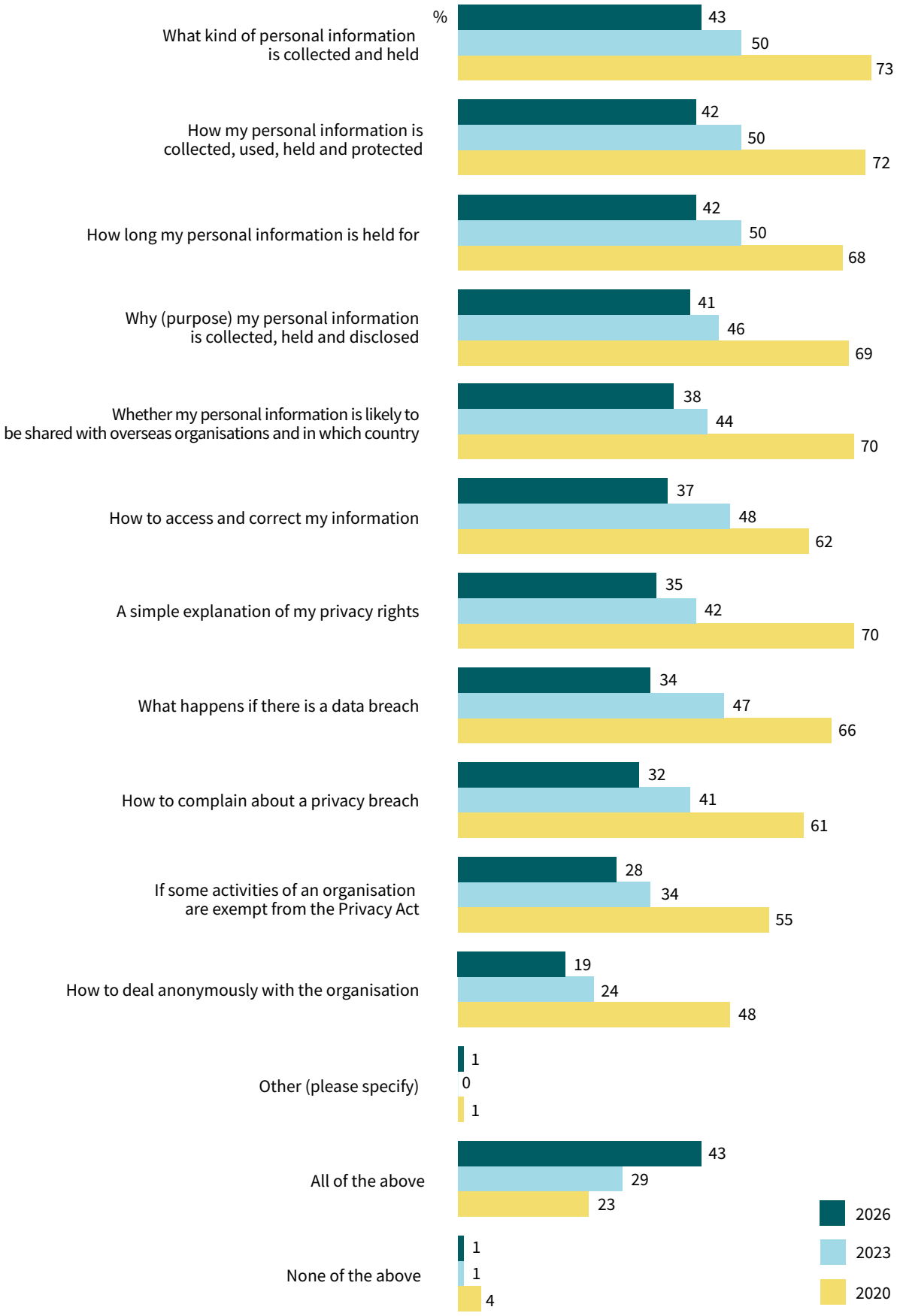
L10. In the past 12 months, how often have you agreed to a company's privacy policy without reading most or all of it?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Australians want a wide range of information included in privacy policies, with more than 2 in 5 (43%) saying all listed information should be included, a continued increase from 2023 (29%) and 2020 (23%). Older Australians aged 50+ are more likely than those aged 18–49 to expect all listed information to be included in privacy policies (49% vs 39%).

Commonly expected inclusions are:

- what kind of personal information is collected and held (43%)
- how personal information is collected, used, stored and protected (42%)
- how long personal information is retained (42%)
- why personal information is collected, held and disclosed (41%)
- whether personal information is likely to be shared with overseas organisations and in which country (38%)
- how to access and correct information (37%)
- a simple explanation of privacy rights (35%)
- what happens if there is a data breach (34%)
- how to complain about a privacy breach (32%)
- if some activities of an organisation are exempt from the Privacy Act (28%)
- how to deal anonymously with the organisation (19%).

Figure 6 Information should be included in all privacy policies



Bar chart segments follow the same top-to-bottom order as the legend

L8. Some people think that privacy policies should be as short as possible, others think they should be comprehensive. With this in mind, which of the following do you think should be in all privacy policies?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653, 2020: n=1,505)
Notes: Don't know (<0.5% in 2026) and refused (0%) not displayed.

Awareness and use of consumer privacy rights

When considering the personal information held by organisations such as banks, energy providers and telecommunications companies, many Australians report limited visibility and control over how their data is managed. Overall, the findings suggest that a substantial proportion of the general community has only partial insight into what personal information organisations hold about them and how it can be accessed.

Two in 5 Australians (40%) report that they do not really know what personal information organisations hold about them or how to access it. A further quarter (24%) indicate they have only partial access, with limited control over their information. These results suggest that clear and effective access to personal information is not consistently experienced across the population.

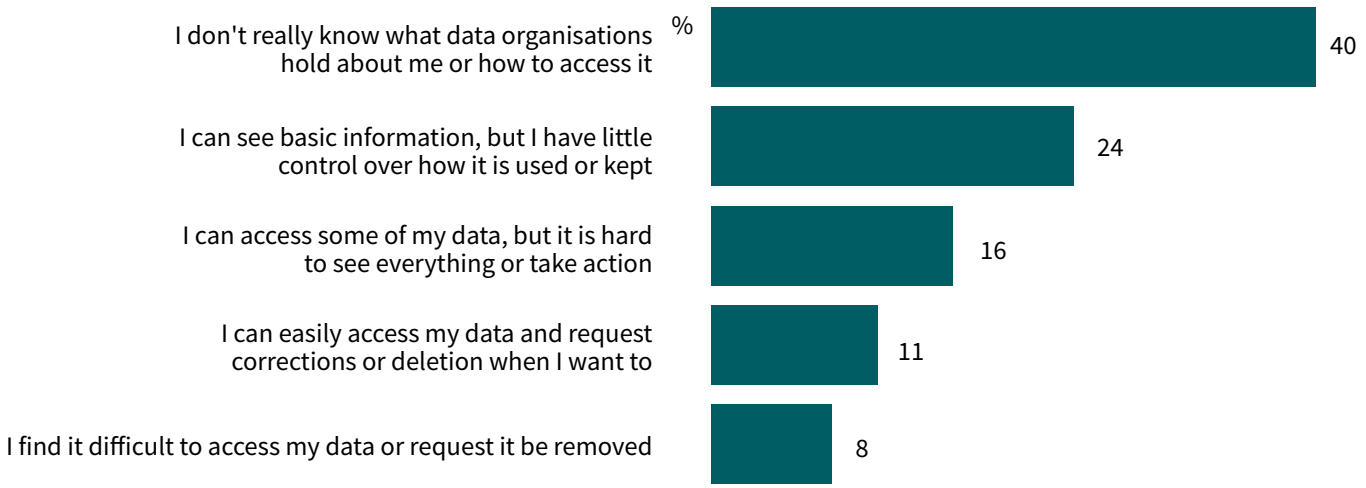
The following groups are more likely to say they do not really know what personal information organisations hold about them or how to access it:

- Australians aged 50+ (46% vs 35% of Australians aged 18–49)
- English-only speakers (43% vs 30% of those who speak a language other than English at home).

Australians who do not really know what personal information organisations hold about them or how to access it are also more likely to:

- be unaware they can request access to their personal information (51% vs 26% of those who are aware)
- say they have never requested access to their personal information (30% vs 12% of people who have requested access).

Figure 7 Experience with organisations holding personal information



L3. Thinking about the personal information organisations hold about you (such as banks, energy providers or telcos), which statement best describes your experience?
Base: All Australians aged 18+. (n=1,504)
Notes: Don’t know (0%) and refused (0%) not displayed.

It is highly relevant then that less than half of all Australians (45%) are aware they have the right to request access to their personal information from organisations, and barely one in 10 (11%) report having done so, consistent with 2023 results.

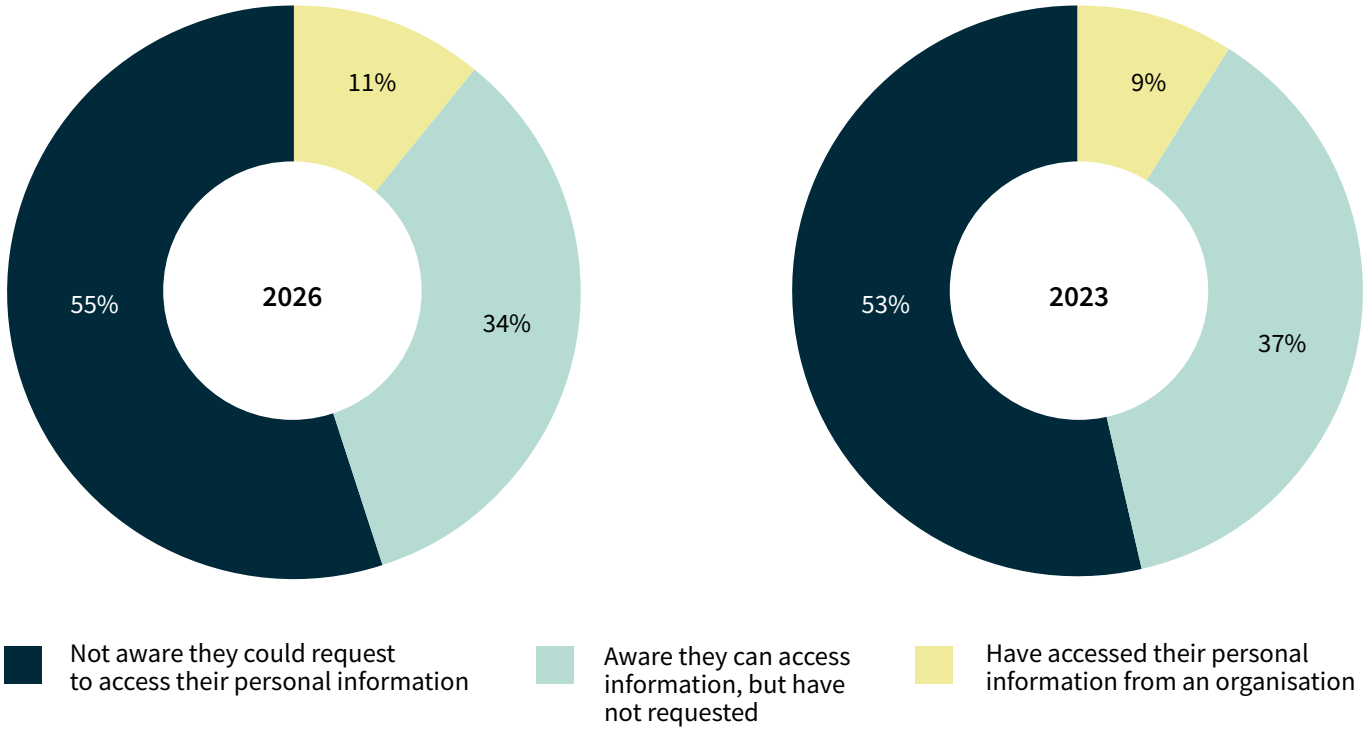
Awareness of this right in legislation is lower among Australians aged 65+ (34% vs 48% of those aged 18–64).

Some groups are more likely to have requested access to their personal information, including:

- Australians aged 18–24, who are around 3 times more likely than those aged 25+ to have done so (27% vs 9%)
- those who speak a language other than English at home (15% vs 9% of English-only speakers).

Australians who are aware of this right, or who have requested access to their personal information, are also more likely to report feeling some or a great deal of control over how their personal information is collected and used.

Figure 8 Access to personal information held by organisations



Pie chart segments follow the legend in an anti-clockwise direction from the left side

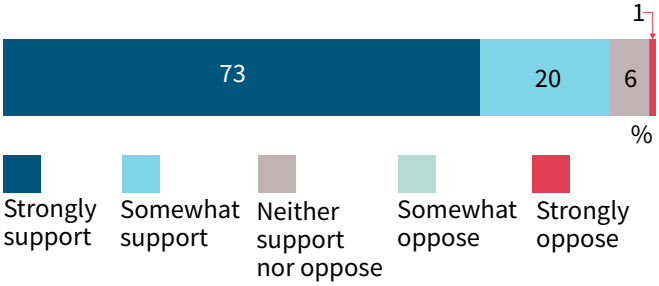
L4. Are you aware that you can request to access your personal information from organisations? L5. Have you ever requested to access your personal information from an organisation?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653)
Notes: Don't know (0%) and refused (0%) not displayed.

Support for data deletion and erasure

Australians show strong support for the right to data deletion and erasure. More than 9 in 10 (93%) support or strongly support a legal right for individuals to request that organisations delete their personal information, including almost three-quarters (73%) who strongly support this provision.

Support is stronger among Australians aged 50+ (97% vs 90% of those aged 18–49), those who are more concerned about their privacy than 5 years ago (94% vs 83% of those less concerned or about the same), and those aware of a data breach in the past 12 months (95% vs 88% of those unaware).

Figure 9 Support for a legal right to request deletion of personal information



Strongly support/somewhat support **93**

Bar chart segments follow the same left-to-right order as the legend

DEL1. How strongly do you support or oppose a legal right for individuals to request that organisations delete their personal information?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

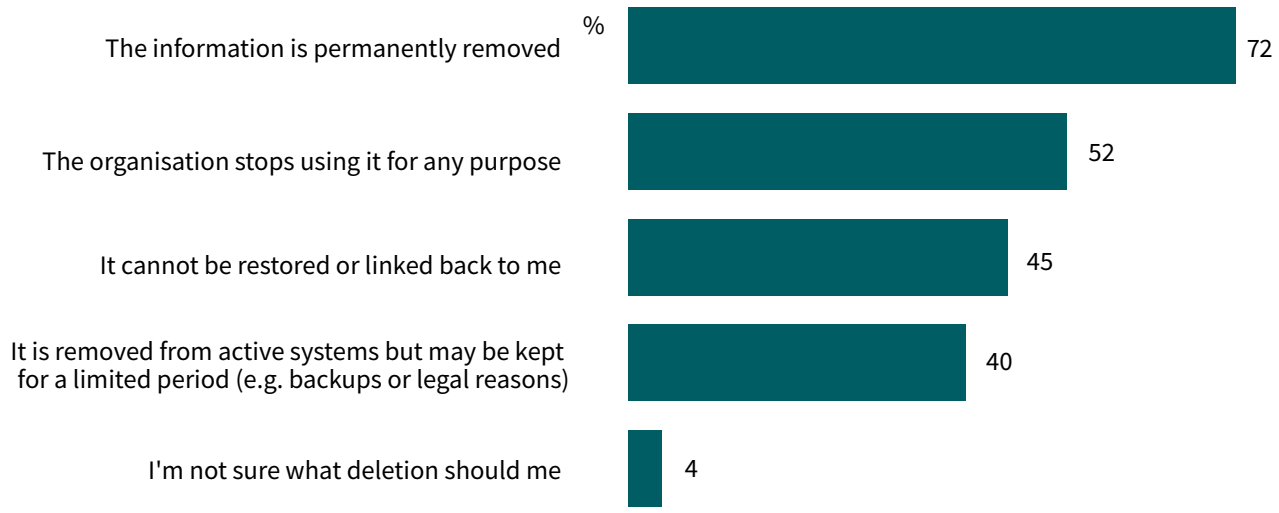
When Australians ask an organisation to delete their personal information, most expect this to result in complete and irreversible removal:

- Around 7 in 10 (72%) expect their information to be permanently deleted.
- Over half (52%) expect the organisation to stop using the information for any purpose.
- Under half (45%) expect that the information cannot be restored or linked back to them.
- Two in 5 (40%) expect information to be removed from active systems but potentially retained for a limited period, such as for backups or legal requirements.

Younger Australians aged 18–34 are more likely than those aged 35+ to expect that deletion of personal information means:

- the organisation stops using it for any purpose (64% vs 47%)
- the information cannot be linked back to them (55% vs 40%)
- the information is removed from active systems, even if retained for a limited period (48% vs 36%).

Figure 10 Expectations when requesting deletion of personal information



DEL2. When you ask an organisation to delete your personal information, what do you expect should happen?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Role of privacy in consumer decision-making

Quality, price and reliability continue to be the primary factors influencing Australians' choice of products and services, although their relative importance has shifted over time. Australians are most likely to rank the following among their top 3 considerations:

- quality of service (63%)
- price (54%, down from 62% in 2023)
- reliability (50%, up from 33% in 2023)
- overall reputation (41%).

While privacy is not a primary driver of choice, it remains an important consideration when choosing products and services. Australians are more likely to rank privacy-related factors than convenience-related factors among their top 3 considerations, suggesting that many Australians may be willing to trade some convenience for stronger privacy protections:

- trust in an organisation's ability to keep personal information secure (33%)
- organisations that collect as little personal information as possible (25%)
- making life easier (20%, down from 25% in 2023)
- speed of access (10%).

The prioritisation of privacy also varies by attitudes and behaviours, and privacy-related decision-making is shaped by broader orientations toward privacy and engagement with information practices.

- Australians who are more concerned about their privacy than 5 years ago are more likely to rank information security among their top 3 factors (34% vs 25% of those with the same or lower level of concern).
- Those who routinely accept privacy policies without reading them are less likely to rank both data security (28% vs 44% of those who read them at least sometimes) and data minimisation (21% vs 33%) among their top 3 considerations.

Australians also place a high and increasing level of importance on how their personal information is collected, used and protected when choosing a product or service.

- Nearly 9 in 10 say it is important their personal information is protected (89%, up from 86% in 2023).
- More than 4 in 5 say it is important they are not asked for more personal information than necessary (85%, up from 81% in 2023).
- More than 4 in 5 say it is important they are clearly told how their personal information will be used (82%, up from 79% in 2023).

Australians aged 50+ are more likely than those aged 18–49 to place high importance on not being asked for more personal information than needed (89% vs 81%). Women are also more likely than men to say that having their personal information protected (69% vs 62%) and being clearly informed about how it will be used (54% vs 46%) are extremely important.

Privacy legislation

Overall, awareness of the Office of the Australian Information Commissioner (OAIC) and the Privacy Commissioner is mixed, with many Australians recognising the name but having limited understanding of its role.

At the same time, there is strong and growing support for strengthening privacy protections. Australians broadly favour extending the Privacy Act obligations to currently exempt sectors and consistently support enhanced individual rights, particularly the right to have organisations delete personal information held about them. Together, these findings highlight a receptive environment for the OAIC to build awareness, reinforce its relevance, and play a more prominent role in shaping public understanding and trust in privacy governance.

Awareness of the Privacy Commissioner

Australians show mixed awareness of the OAIC. Nearly half of the Australian community (49%) are aware of the OAIC. Only one in 10 (9%) say they are familiar with its role.

In 2023, fewer people – just under 2 in 5 (38%) – were aware that the OAIC exists to uphold privacy laws and investigate complaints about the misuse of personal information. However, due to differences in question framing, the results are not directly comparable across years.

Awareness of the OAIC is higher among:

- older Australians aged 55+ (59% vs 40% of those aged 18–45)
- English-only speakers (53% vs 36% of those who speak a language other than English at home).

Support for changes to the Privacy Act

There is strong support among Australians for extending Privacy Act obligations to sectors that are currently exempt, suggesting broad expectations that personal information should be handled consistently across the economy.

Support is highest for applying the same privacy standards to:

- businesses collecting employee data, including monitoring or surveillance (89% vs 81% in 2023, 73% in 2020)
- political parties and representatives (88% vs 82% in 2023, 74% in 2020).

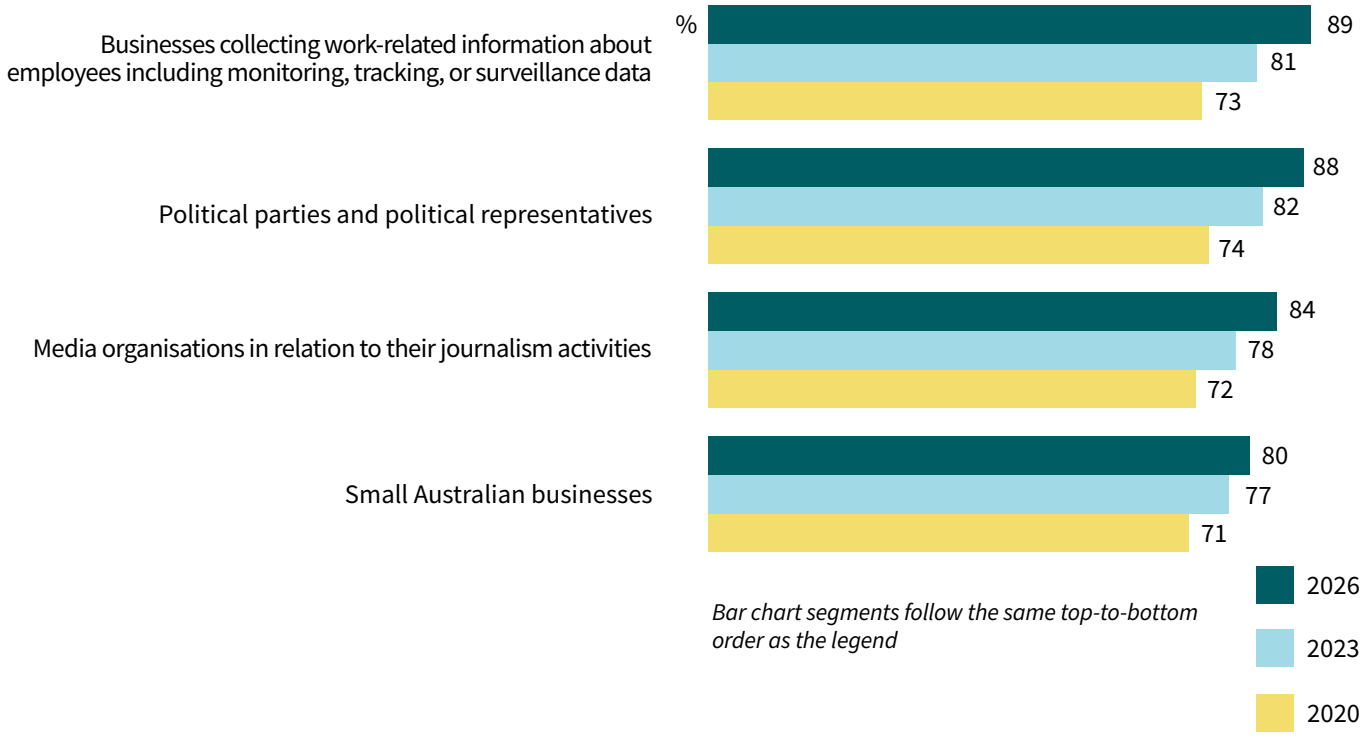
Support remains high for extending privacy regulation to:

- media organisations (84% vs 78% in 2023, 72% in 2020)
- small Australian businesses (80% vs 71% in 2020).

Women are consistently more likely than men to support applying the same privacy standards across sectors, including:

- businesses collecting work-related employee information (91% vs 86%)
- political parties and representatives (91% vs 86%)
- media organisations (87% vs 82%)
- small Australian businesses (84% vs 76%).

Figure 11 Belief that organisation types should be covered by the Privacy Act

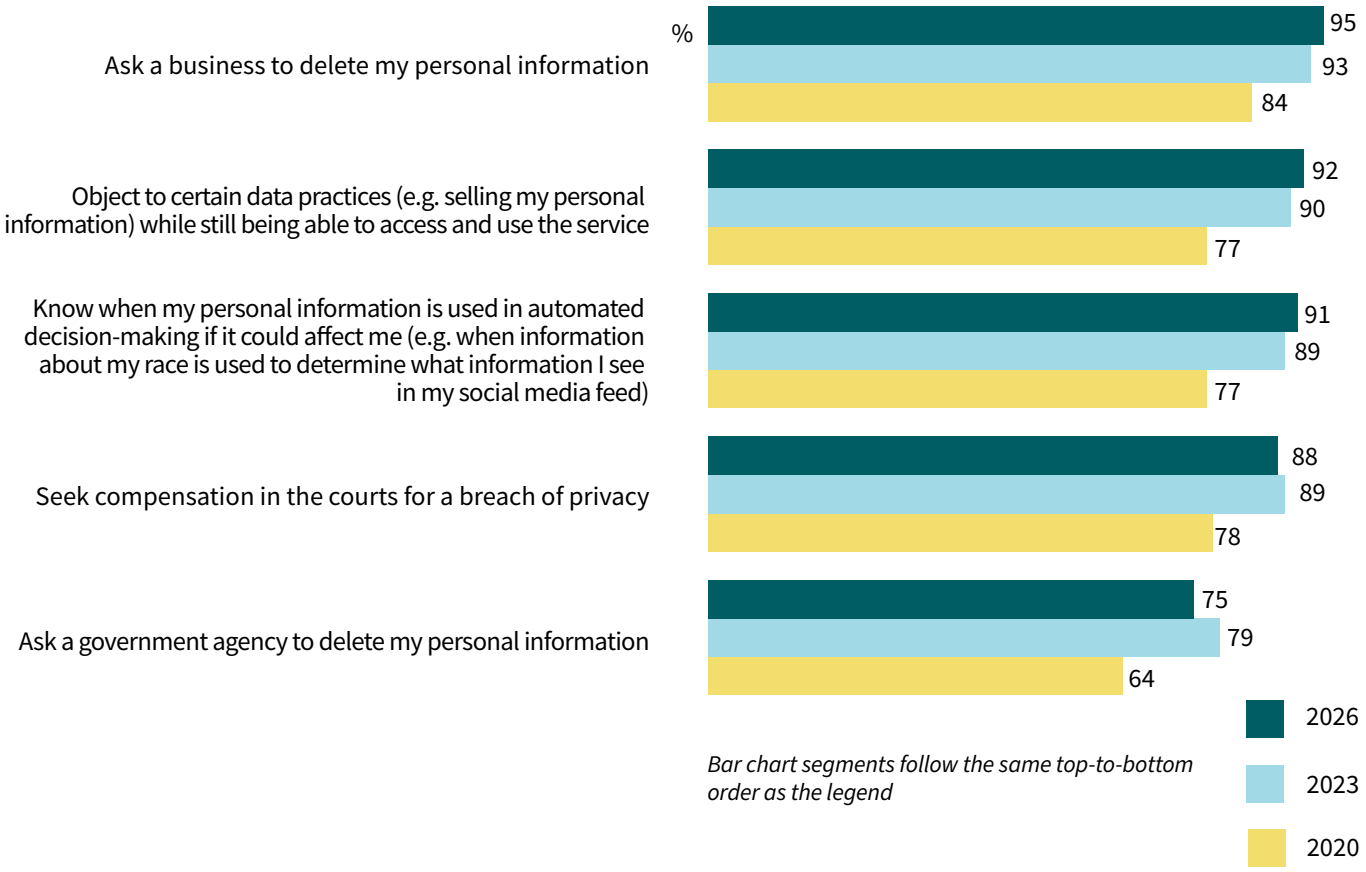


L2. The following sectors are currently exempt from the Australian Privacy Act. Should they have to handle your personal information in the same way as government agencies and larger businesses?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653, 2020: n=1,509)
Notes: Don't know (0%) and refused (all <0.5%) not displayed.

Australians strongly support the introduction of additional individual rights under the Privacy Act, including the right to:

- ask a business to delete their personal information (95%, up from 93% in 2023)
- object to certain data practices while continuing to access services (92%)
- be informed when their personal information is used in automated decision-making (91%)
- seek compensation for a breach of privacy (88%).
- request that government agencies delete their personal information (75%, down from 79% in 2023).

Figure 12 Specific rights should be included under the Australian Privacy Act

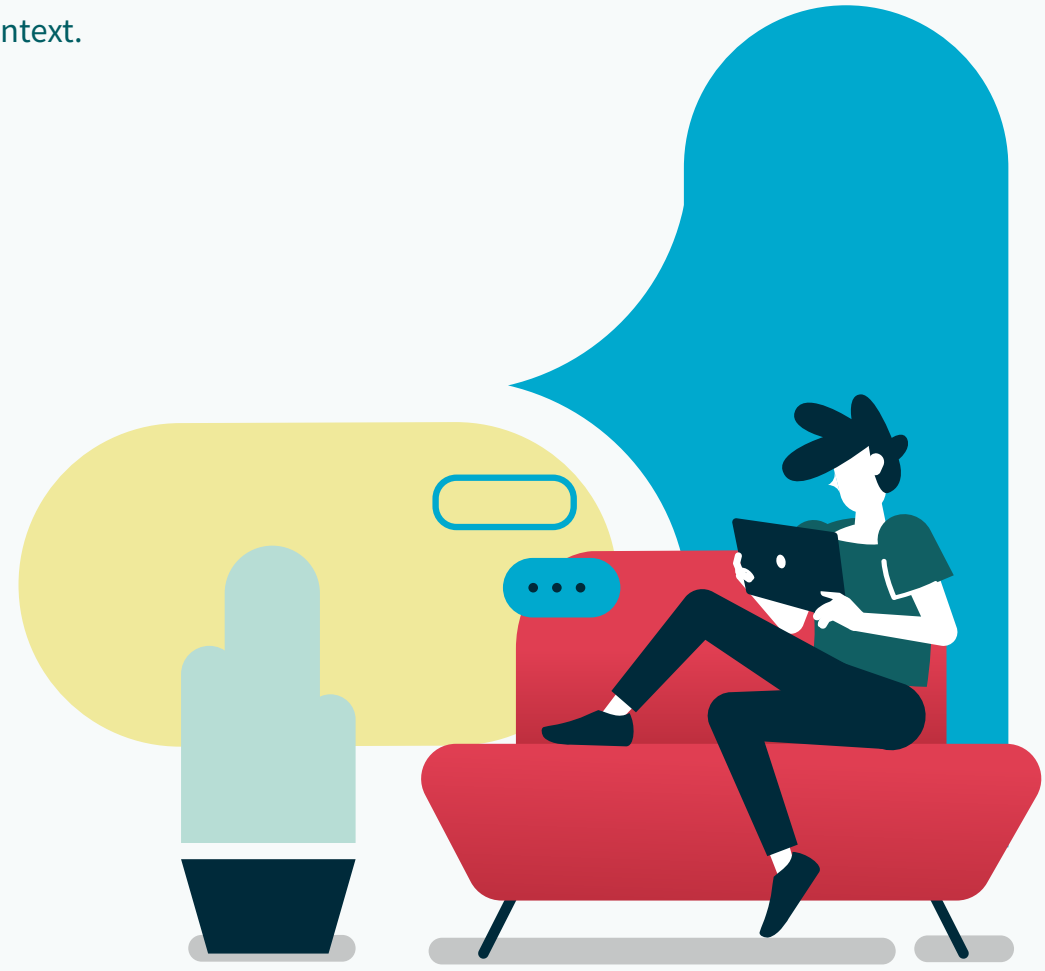


L6. Do you believe you should have these rights under the Australian Privacy Act?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653, 2020: n=1,509)
Notes: Don't know (1% in 2026, between 8% and 11% in 2023, between 16% and 17% in 2020) and refused (all <0.5% in 2026) not displayed.

The role of organisations

Trust in organisations to protect and use personal information varies markedly by sector, with strongest confidence in essential and public-facing services such as health, government and financial institutions. Weaker trust was recorded in commercial, digital and data-driven industries including AI, social media companies and data brokers. At the same time, Australians are becoming more selective about what personal information they consider fair to share, generally limiting acceptance to basic details and situations where there are a clear purpose and a trusted context.

This cautious approach also extends to government data use, where Australians are more comfortable when information is used to deliver services or public benefit, but less accepting of practices that lack transparency, involve identifiable data, or are not clearly communicated, highlighting the importance of trust, purpose and control.



Trustworthiness of organisations by sector

Trust in organisations to protect and appropriately use personal information varies markedly by sector.

Health service providers are the most trusted industry sector, with 74% of Australians viewing them as trustworthy. Trust is also higher for sectors linked to public services and regulated handling of personal information, including:

- government agencies (68%)
- financial institutions (59%)
- education providers (57%, down from 61% in 2023).

Trust is more mixed across some commercial sectors, with confidence declining over time in several industries:

- insurance companies (28%, down from 40% in 2023)
- telecommunications providers (24%, down from 37% in 2023)
- technology companies (17%, less than half of 39% in 2023).
- real estate agencies (13%, nearly half of 23% in 2023)
- retailers (10%, around a third of 30% in 2023).

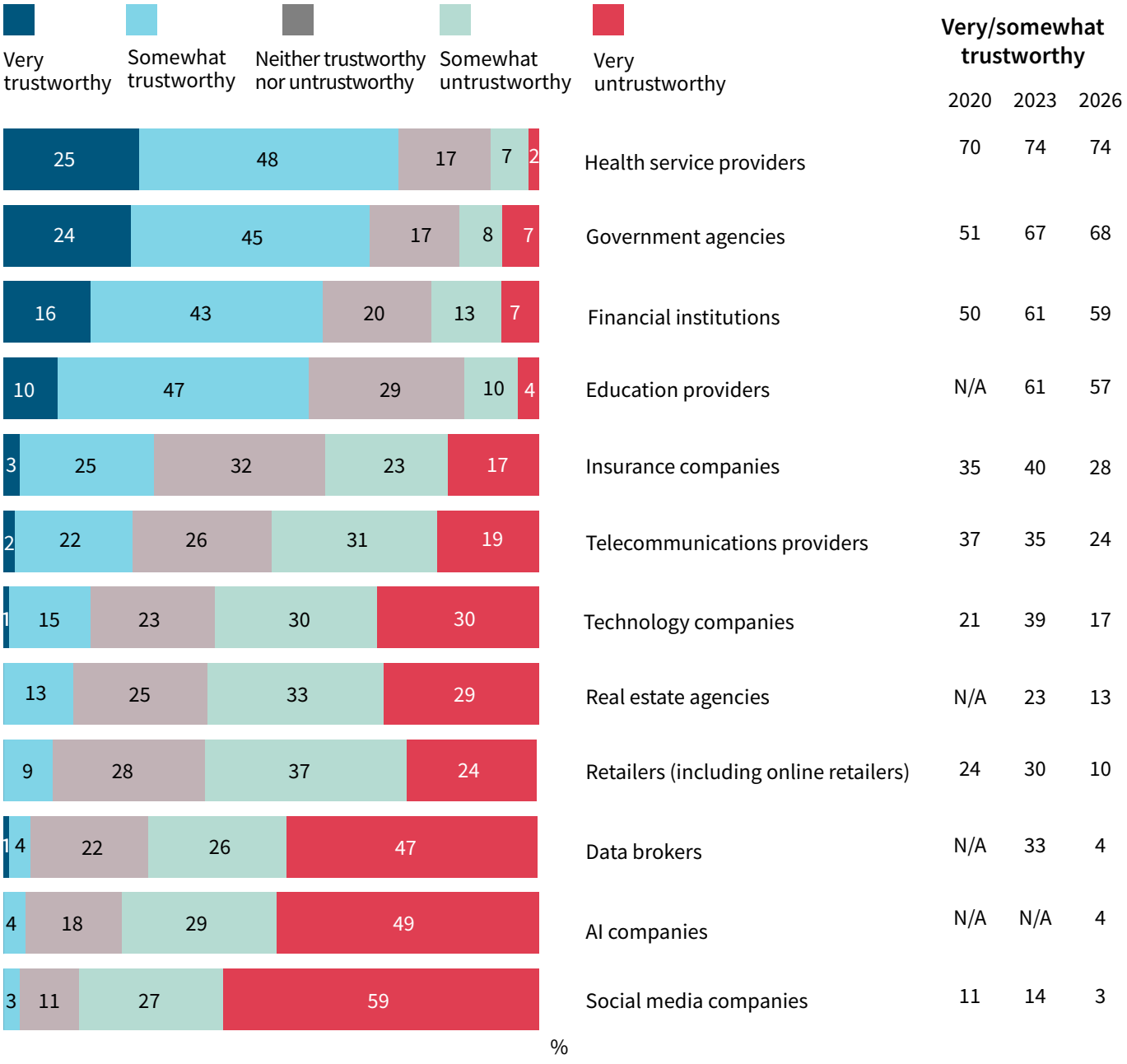
The lowest levels of trust are reported for data-driven sectors whose core activities involve large-scale data collection and analysis:

- data brokers (4%)
- AI companies (4%)
- social media companies (3%, down from 14% in 2023).

Trust and distrust also vary across population groups:

- Australians aged 65 and over are more likely than those aged 18–64 to trust telecommunications providers (35% vs 21%).
- Men are more likely than women to view data brokers (78% vs 69%), real estate agencies (66% vs 57%), and insurance companies (44% vs 37%) as untrustworthy, while women are more likely than men to trust education providers (61% vs 53%).

Figure 13 Trust in organisations to protect and use personal information



Bar chart segments follow the same left-to-right order as the legend

F1. Thinking now about trustworthiness, how trustworthy would you say the following organisations are with regard to how they protect and use your personal information?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,642, 2020: n=1,505)
Notes: Very trustworthy for Real estate agencies, Retailers (including online retailers), AI companies and Social media companies are all <0.5%. Don't know (all <1%) and refused (all <0.5%) not displayed. "Credit reporting bodies (e.g. Equifax, Illion, Experian)" label was updated to "Data brokers (e.g. Acxiom, Experian Marketing Services, Quantium, companies that buy and sell consumer data)" in 2026, so comparisons with 2023 should be interpreted with caution.

Expectations of fair and reasonable data collection by sector

Respondents were shown a list of different types of personal information and asked what they considered fair and reasonable to provide when accessing services in specific sectors. Compared with 2023, the proportion of Australians who say none of the listed types of personal information are fair and reasonable to provide has doubled (12%, up from 6%), suggesting growing caution about sharing personal information when accessing services across industries.

Australians are most likely to consider basic contact and identity information fair and reasonable to provide, including:

- email address (85%)
- name (85%, down from 90% in 2023)
- phone number (78%, down from 82%)
- date of birth and address (both 72%, down from 78%)
- identification documents (e.g. driver's license, passport) (52%).

Acceptance has declined for the collection of more sensitive or behavioural data:

- data on how they access, use or interact with services (35%)
- marital status (32%, down from 38%)
- Medical or health information (31%)
- financial information (29%, up from 25%)
- location data (28%).

The lowest levels of acceptance are for highly sensitive or intrusive data, including:

- sexual orientation and biometric information (e.g. fingerprints, facial images) (both 11%)
- social media identifiers (e.g. profile links, usernames, social media activity) (10%)
- religion (9%)
- behavioural or psychological data about interests, habits, likes and dislikes (8%)
- detailed website or app tracking data (e.g. pages viewed, clicks, browsing behaviour across sites) (7%).

Men are more likely than women to consider biometric information being fair and reasonable to provide (14% vs 8%). Younger Australians aged 18–24 are more likely to view social media identifiers as acceptable (24% vs 8% of those aged 25+), while those aged 65+ are more likely to consider location data fair and reasonable (38% vs 25% of those aged 18–24).

Across sectors, basic contact and identity information, such as email address and name, are the most widely accepted data types to provide, particularly for financial institutions, government agencies and health service providers, where additional information such as phone number and date of birth are also commonly seen as reasonable, and more sensitive data aligns with context (e.g. financial information for banks and health information for healthcare providers). Telecommunications and insurance providers follow a similar but slightly lower pattern, with strong acceptance of core details but more limited acceptance of sensitive data. In contrast, retailers and real estate agencies see lower acceptance beyond basic contact information, while technology companies and social media platforms have the narrowest acceptance overall, with users largely restricting what they consider reasonable to share and showing comparatively higher resistance across most data types.

Figure 14 Information considered fair and reasonable to provide when accessing services by industry sector

	Financial institutions	Government agencies	Health service providers	Retailers	Social media companies	Telecom-munications providers	Technology companies	Insurance companies	Real estate agencies
Email address	89%	88%	86%	84%	80%	87%	82%	87%	82%
Name	89%	91%	90%	78%	81%	85%	81%	86%	81%
Phone number	86%	83%	87%	72%	66%	86%	69%	80%	76%
Date of birth	83%	89%	89%	61%	66%	69%	62%	76%	60%
Address	83%	86%	81%	69%	54%	74%	61%	74%	65%
Identification documents	71%	75%	56%	41%	34%	51%	35%	54%	48%
Data on how I access, use or interact with their service	39%	41%	37%	34%	33%	35%	35%	35%	31%
Marital status	38%	56%	39%	24%	25%	22%	24%	31%	30%
Medical or health information	23%	37%	88%	21%	18%	20%	20%	41%	18%
Information about my finances	61%	39%	21%	21%	21%	21%	17%	26%	31%
Location data	28%	27%	31%	23%	24%	35%	27%	30%	27%
Household composition	25%	36%	22%	21%	21%	17%	16%	29%	31%
Sexual orientation	9%	13%	26%	9%	12%	7%	11%	7%	7%
Biometric information	20%	15%	12%	7%	10%	8%	11%	8%	7%
Social media identifiers	9%	10%	7%	7%	27%	8%	13%	6%	6%
Religion	7%	15%	17%	6%	9%	6%	9%	6%	9%
Behavioural or psychological data about my interests, habits, likes and dislikes	8%	5%	15%	9%	10%	7%	11%	7%	4%
Detailed website or app tracking	5%	5%	5%	9%	9%	8%	8%	5%	7%
None of the above	8%	12%	7%	13%	22%	8%	14%	8%	15%

Less fair/reasonable — More fair/reasonable

F2. What information would you consider to be fair and reasonable to provide to when accessing their services? (Merged F2A, F2B) Base: Financial institutions (n=339), Government agencies (n=322), Health service providers (n=330), Retailers (n=336), Social media companies (n=333), Telecommunications providers (n=335), Technology companies (n=328), Insurance companies (n=342), Real estate agencies (n=343). Notes: Prefer not to say (0%) and unsure (all <0.5%) not displayed.

Comfort with government use of personal information and data linking

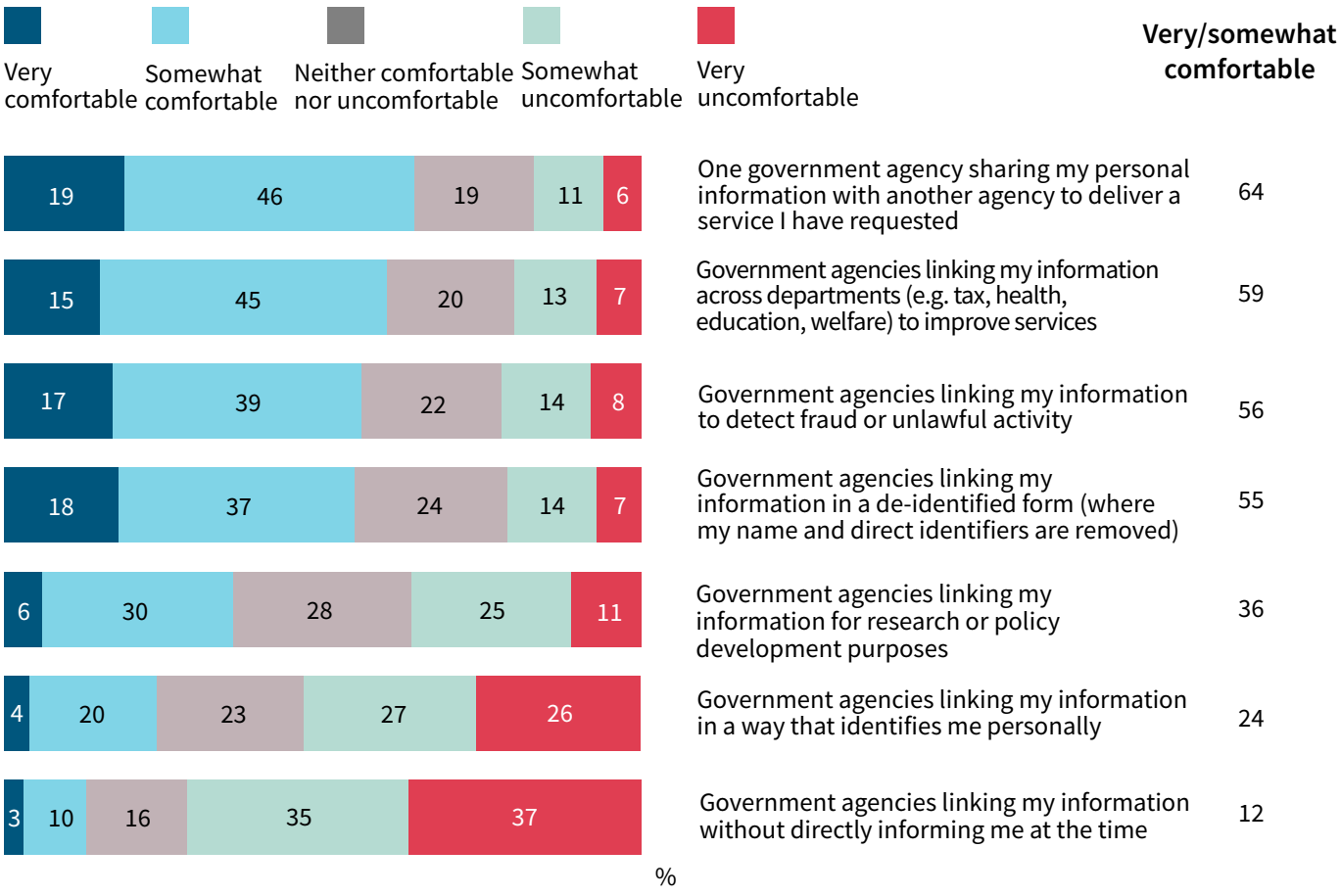
Australians are more comfortable with cross agency data use when it is framed around service delivery, improvement, safety, or de-identification. Australians are more likely to feel comfortable or very comfortable with:

- sharing information with another agency to deliver a requested service (64%)
- agencies link information across departments to improve services (59%)
- linking information to detect fraud or unlawful activity (56%)
- linking information to be used in a de-identified form (55%).

Comfort declines when the purpose is research or policy development, with only 36% feeling comfortable. Views are more divided in this context, suggesting uncertainty or mixed acceptance when data use is less directly connected to immediate personal benefit, public good or clear protections. Australians are least comfortable with practices that reduce transparency or increasing identifiability:

- Only one-quarter (24%) are comfortable with government agencies linking information in a way that identifies them personally.
- 72% feeling uncomfortable when linking occurs without directly informing the individual at the time.

Figure 15 Comfort with government agencies' use of personal information



Bar chart segments follow the same left-to-right order as the legend

F7. How comfortable are you with the following uses of your personal information by government agencies?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (all <0.5%) and refused (0%) not displayed.

Privacy concerns and dispute resolutions

Privacy concerns are widespread and increasing in Australia, yet relatively few people take action when issues arise, often due to low confidence in outcomes and perceived complexity of complaints processes. Experiences are commonly linked to direct marketing, unnecessary data collection, and limited transparency, with complaint processes frequently seen as difficult and rarely leading to satisfactory outcomes. Confidence in how organisations handle privacy complaints is stronger in traditional sectors such as banking, health, and government than in social and digital platforms.

Although fewer people know about or have personally experienced data breaches, most people who are affected still report harm. The most common harms are more scams and spam, as well as loss of trust, less control, and ongoing concern about how their personal information is used.

Australians prioritise limiting data collection and timely deletion as the most important ways organisations should protect personal information, and place primary responsibility for privacy risks on organisations. There is strong expectation that organisations should lead in preventing issues, while responsibility for addressing problems is more shared with government and regulators.

Experiences of privacy concerns

About 2 in 3 Australians (64%) have had concerns about how an organisation handled their personal information. This ranges from relatively minor issues, such as being asked for unnecessary information, to more serious incidents like data breaches. However, only around one in 8 (12%) say they raised the issue with the organisation. Australians who had concerns but didn't raise them are more likely to be men (56% vs 49% of women) and live in metropolitan areas (55% vs 46% of those outside capital cities).

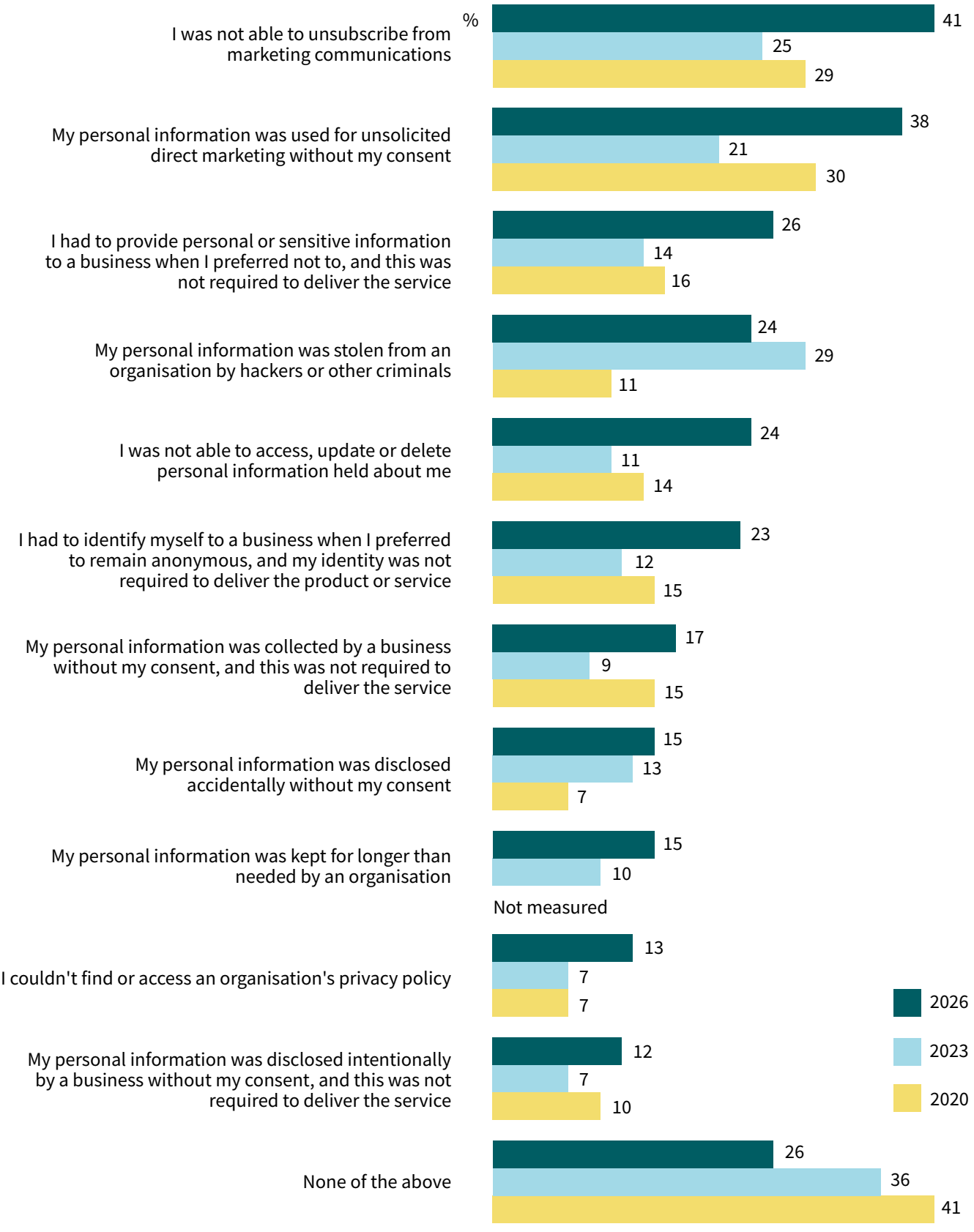
When asked separately about a list of specific privacy-related experiences (Figure 16) in the past 12 months, around 3 in 4 (73%) Australians report experiencing at least one issue, up from 64% in 2023. This measure captures a broader range of experiences, which respondents may not necessarily view as a broader concern about how an organisation handled their personal information.

The most common experiences relate to direct marketing, including difficulties unsubscribing and receiving unsolicited communications, followed by being asked to provide unnecessary personal information. A substantial proportion also report issues relating to data breaches, limited ability to access or manage their information, and being required to identify themselves when it was not necessary. Experiences of unauthorised collection, use, or disclosure of personal information, as well as difficulties accessing privacy policies, are also reported by a notable minority.

Experiencing at least one privacy-related issue is more likely among:

- those with tertiary or vocational qualifications (77% vs 60% of those with no qualification)
- those who are more concerned about their privacy than 5 years ago (75% vs 59% of those with the same or lower level of concern)
- those who have concerns about how organisations handle their personal information (82% vs 58% of those with no concern)
- those aware of data breaches in Australia in the past 12 months (79% vs 57% of those unaware).

Figure 16 Problems experienced with the handling of personal information



Bar chart segments follow the same top-to-bottom order as the legend

P3. Have you experienced any of the following in the past 12 months?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,626, 2020: n=1,509)
Notes: Don't know (1%) and refused (<0.5%) not displayed.

Barriers to raising privacy complaints

Many people who were worried about how an organisation handled their personal information didn't end up making a complaint. The main reasons were that they:

- didn't think it would change anything (56%)
- thought it would be too hard or take too long (51%)
- weren't sure how to complain (40%).

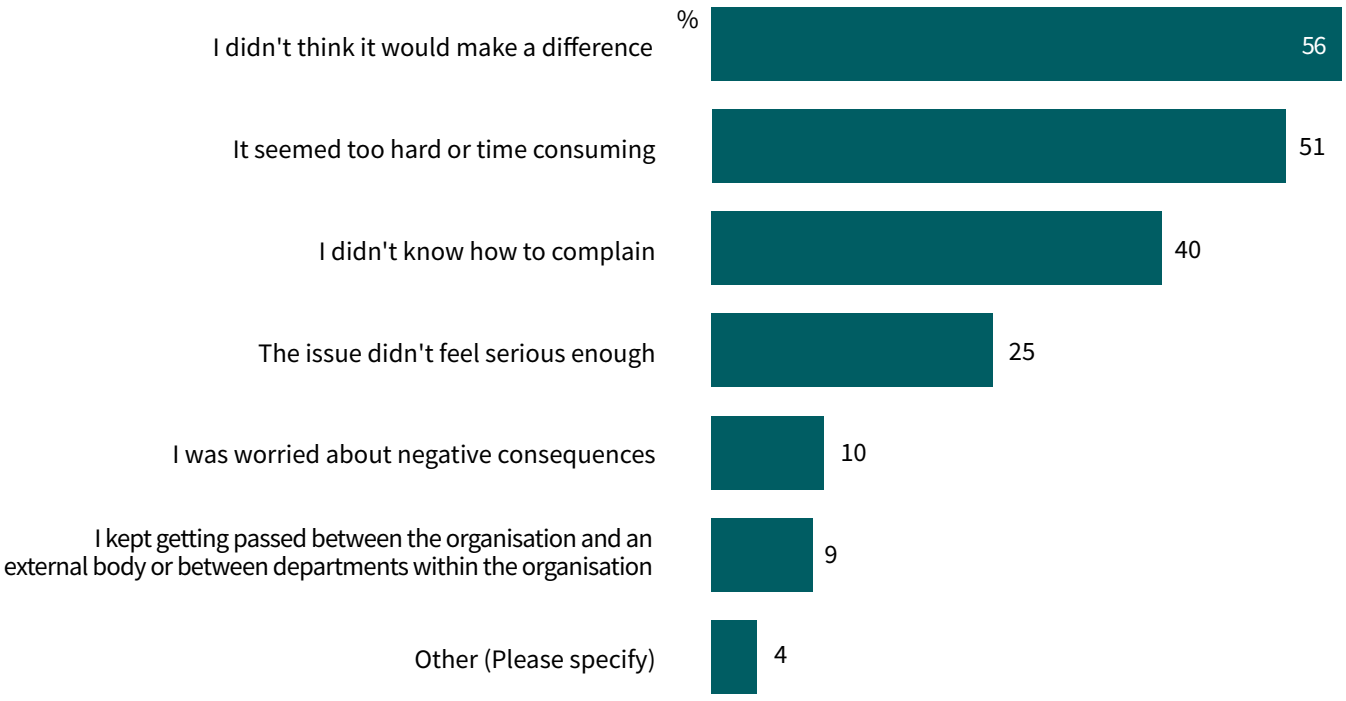
These barriers were even more common for people aged 18–49. Compared with people aged 50+, younger Australians were more likely to say they didn't complain because:

- it felt too hard or time-consuming (58% vs 41%)
- they didn't know what to do or where to start (48% vs 31%).

People with a university qualification were also more likely to feel the process was too difficult or time-consuming (63%), compared with those with vocational qualifications (46%) or no qualifications (42%). And people who speak a language other than English at home were more likely to say the process felt too hard (60% vs 47%).

Lower complaint rates may also reflect broader challenges around awareness, confidence and perceived ability to exercise privacy rights. Australians who are unaware they can request access to their personal information from organisations are more likely not to raise a complaint after experiencing a concern (56% vs 48% of those aware of this right). More broadly, Australians who do not pursue complaints are also more likely to report limited understanding of how organisations use their personal information, lower perceived control over how their data is collected and used, and a belief that consent and data sharing are rarely genuine choices. They are also more likely to perceive current data practices as unfair in practice. Combined with concerns about effort, complexity and ineffective outcomes, these findings may reflect broader feelings of low agency and limited confidence that engaging with complaint processes or exercising privacy rights will lead to meaningful resolution or change.

Figure 17 Reasons for not pursuing a privacy complaint



COM2. If you decided not to pursue a privacy complaint, what were the main reasons?
Base: Had a concern about how personal information was handled but did not raise it with the organisation (n=790)
Notes: Don't know (<0.5%) and refused (<0.5%) not displayed.

Perceived effectiveness of complaint handling

Perceived effectiveness of privacy complaint handling varies sharply by sector.

Australians most commonly identify banks and financial institutions (46%), health services (42%) and government agencies (41%) as handling privacy complaints fairly and effectively, while confidence is very low in online retailers (4%) and social media platforms (3%). Taken together, the results suggest that perceived 'effective complaint handling' is largely associated with a small set of essential or institutionally familiar sectors, whereas many Australians do not see strong pathways for redress in more commercial or digital environments. This is reinforced by the fact that almost 3 in 10 (29%) believe that none of the listed organisations handle privacy complaints fairly and effectively.

Men are more likely than women to perceive the following sectors handle privacy complaints fairly and effectively, which may indicate slightly higher confidence (or lower scepticism) among men in the responsiveness of these sectors.:

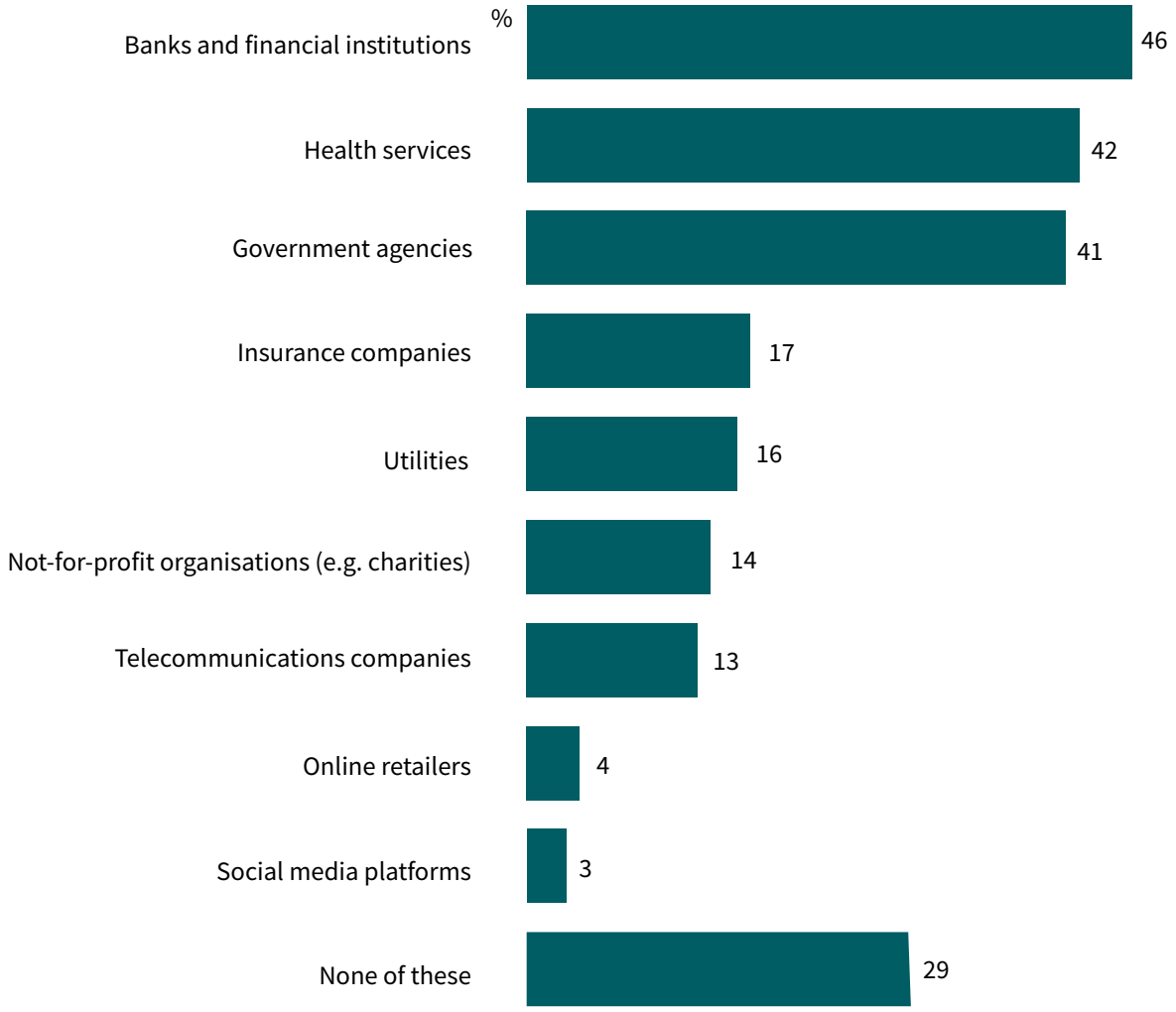
- government agencies (43% vs 38%)
- telecommunications companies (16% vs 10%)
- online retailers (6% vs 3%).

Australians aged 65 and over are more likely than younger people to say that some sectors handle privacy complaints fairly and effectively, including:

- banks and financial institutions (55% vs 39% of those aged 18–34)
- health services (50% vs 38% of those aged 25–64)
- utilities (23% vs 12% of those aged 18–49).

This may reflect greater familiarity with traditional service providers, or a stronger sense that these organisations are accountable, rather than higher confidence in complaint handling overall.

Figure 18 Organisations perceived to handle privacy complaints fairly and effectively



COM3. Which types of organisations do you think generally handle privacy complaints fairly and effectively?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (2%) and refused (<0.5%) not displayed.

Experiences of making privacy complaints are often challenging, difficult to navigate and rarely result in satisfactory outcomes. For many complainants the process may feel more like an information exchange than an effective pathway to resolution. This suggests that people judge complaint handling not just by the final outcome, but also by how easy the process is to deal with. For example, being passed around, having to repeat information, and long delays may help explain why few people report a positive experience from start to finish.

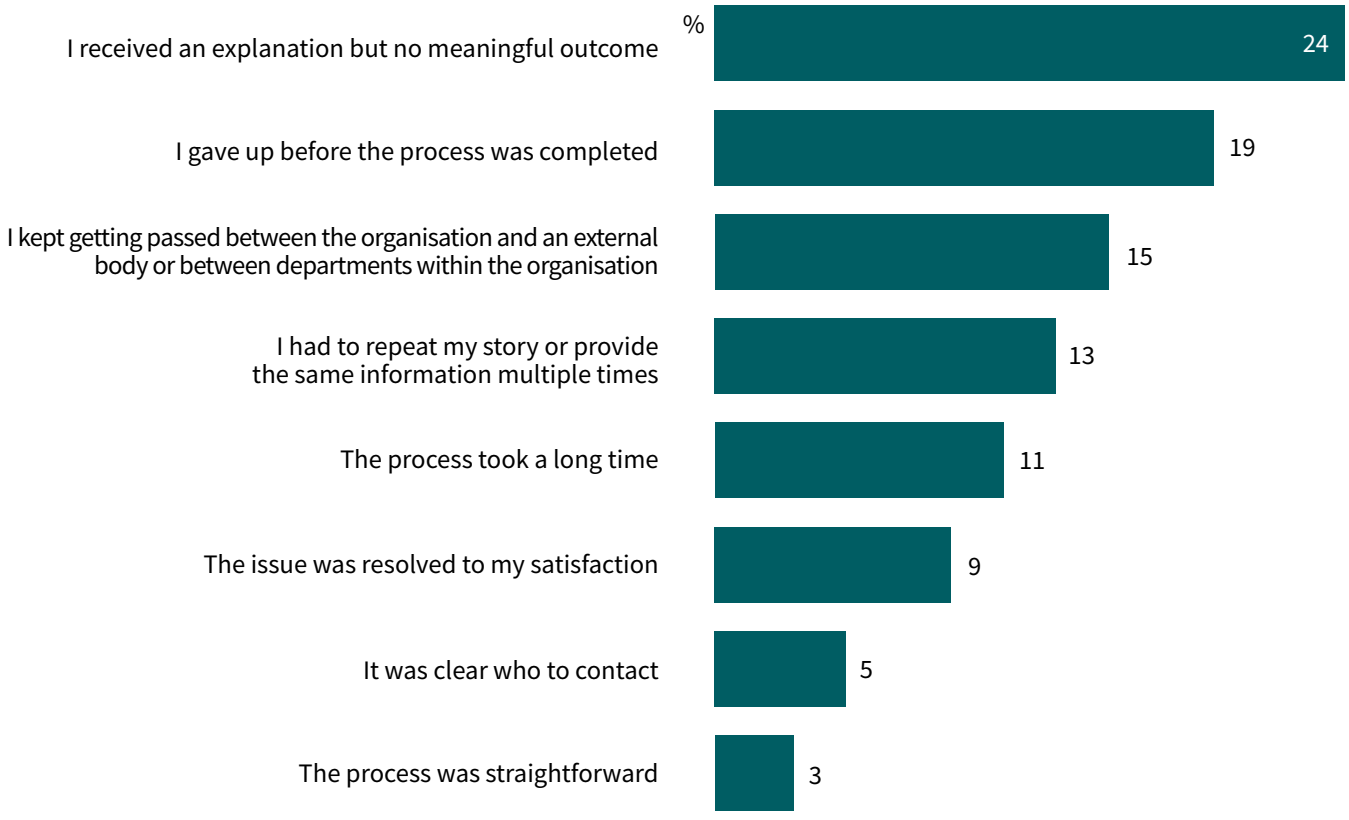
The most common experiences include:

- receiving an explanation without a meaningful outcome (24%)
- giving up before the process was completed (19%)
- being passed between organisations or departments (15%).

Relatively few Australians report positive experiences:

- having their issue was resolved to their satisfaction (9%)
- it was clear who to contact (5%)
- the process was straightforward (3%).

Figure 19 Experience of the most recent privacy complaint



COM4. Thinking about the most recent time you complained about how your personal information was handled, which of the following best describes your experience?
Base: Raised a concern with the organisation about how personal information was handled (n=173)
Notes: Don't know (2%) and refused (0%) not displayed.

Awareness and experience of data breaches

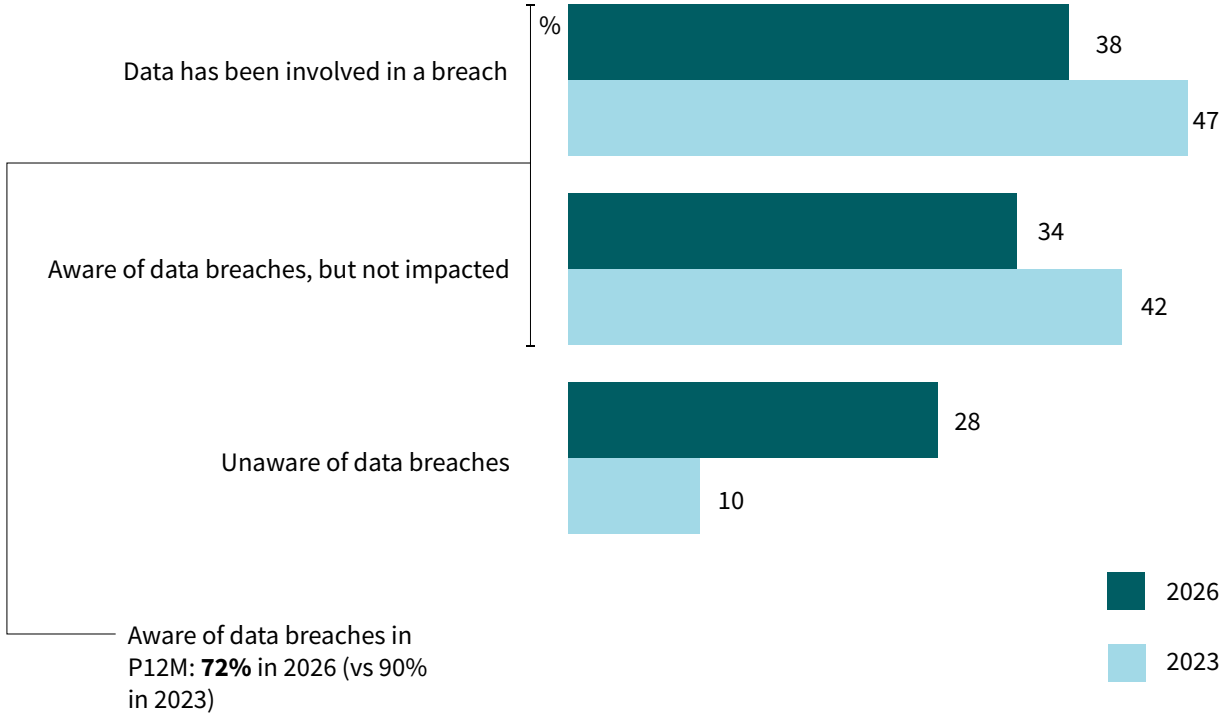
For the purposes of evaluating data breaches, respondents were provided with the following definition of a data breach:

A data breach is a type of privacy breach that occurs when personal information held by an organisation is accessed or disclosed without authorisation, or is lost. Data breaches may result from malicious action (e.g. cyber criminals), human error (e.g. personal information being emailed to the wrong person) or errors in business or technology processes.

Awareness and experience of data breaches in Australia has declined since 2023.

- Around 7 in 10 (72%, down from 90% in 2023) Australians say they heard of a data breach in the past 12 months before the survey.
- Under 2 in 5 (38%, down from 47% in 2023) say they were directly notified by an organisation that their personal information was involved in a breach.
- One in 3 (34%, down from 42% in 2023) reports being aware of breaches but not personally affected.

Figure 20 Awareness and impact of data breaches in the last 12 months



Bar chart segments follow the same top-to-bottom order as the legend

P9. Are you aware of any data breaches occurring in Australia in the last 12 months? P10. In the past 12 months, has an organisation told you that your information was involved in a data breach?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,626)
Notes: Don't know (<0.5% in 2026, 5% in 2023) and refused (0%) not displayed.

It is worth noting that the 2023 survey was conducted in the immediate aftermath of the Optus and Medibank data breaches (September–October 2022), 2 of the largest and most publicly reported data breaches in Australian history. The extraordinary level of media and public attention these incidents generated may have artificially inflated awareness levels at that point in time.

According to OAIC data, reported data breaches in Australia have increased since 2022, with 2024 recording the highest number of notifications since the Notifiable Data Breaches (NDB) scheme commenced in 2018. In 2022, the OAIC received a total of approximately 890 notifications, rising to 1,113 in 2024 – a 25% increase.[2,3] The most recent reporting period (January to June 2025) recorded 532 notifications, which, while representing a 10% decrease on the preceding 6 months, remains consistent with the levels seen throughout 2024.[4] It is worth noting, however, that the second half of 2022 saw a marked spike in notifications, up 26% on the first half of that year, which the OAIC itself attributed in part to the high public profile of the Optus and Medibank breaches, noting that significant public interest in those incidents 'may have raised awareness of the requirement for entities covered by the Privacy Act to notify the OAIC'.[5] This suggests that the period immediately following those landmark breaches represented an atypical peak in reporting activity, and that any comparisons between 2022–23 survey data and later periods should take this into account.

Around 3 in 4 (77%) Australians whose data was involved in a breach report experiencing at least one form of harm, consistent with 2023 (76%). The most common impact is increased exposure to scams and spam, reported by 3 in 5 (62%), marking a notable rise from 2023 (52%). More serious direct impacts are less prevalent but have increased in some cases, including:

- financial or credit fraud (16%, up from 11% in 2023)
- email account hijacked (12%)
- the need to replace key identity documents (12%, down from 29%)
- emotional or psychological harm (10%).

The finding that breach-related harm is increasingly experienced as ongoing digital exposure (such as scams and spam) alongside a smaller but material share experiencing more acute impacts lends support to cross-portfolio collaboration being increasingly relevant.

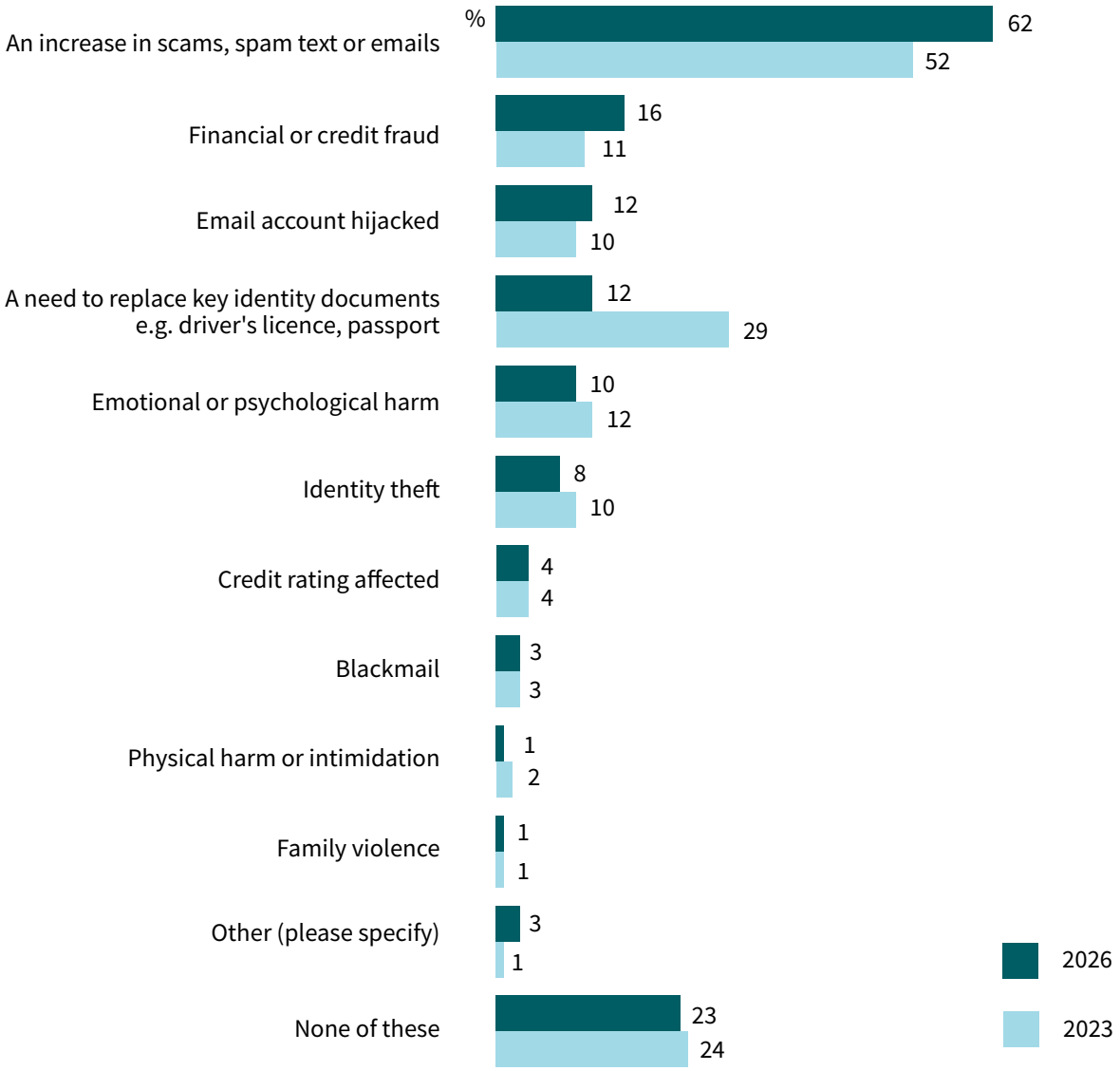
2 OAIC, Notifiable Data Breaches Report: July to December 2022, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2022

3 OAIC, OAIC stats show record year for data breaches, https://www.oaic.gov.au/news/media-centre/oaic-stats-show-record-year-for-data-breaches

4 OAIC, Notifiable Data Breach statistics dashboard, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breach-statistics-dashboard

5 https://www.oaic.gov.au/__data/assets/pdf_file/0026/39068/OAIC-Notifiable-data-breaches-report-July-December-2022.pdf

Figure 21 Personal experiences following an organisational data breach



Bar chart segments follow the same top-to-bottom order as the legend

P12. Which, if any, of the following have you personally experienced because of a data breach of an organisation?
Base: All Australians aged 18+. (2026: n=566, 2023: n=760)
Notes: Don't know (1% in 2026) and refused (<0.5% in 2026) not displayed.

Harms resulting from privacy breaches

Among Australians who experienced a problem with how their personal information was handled in the 12 months prior to the survey, 9 in 10 (91%) report at least one type of harm, a slight decline from 2023 (96%).

The most common and increasing impact is an increase in scams or spam (70% vs 55% in 2023), consistent with experiences following data breaches, suggesting that privacy problems are often experienced as sustained digital exposure rather than a one-off event.

Other common impacts include:

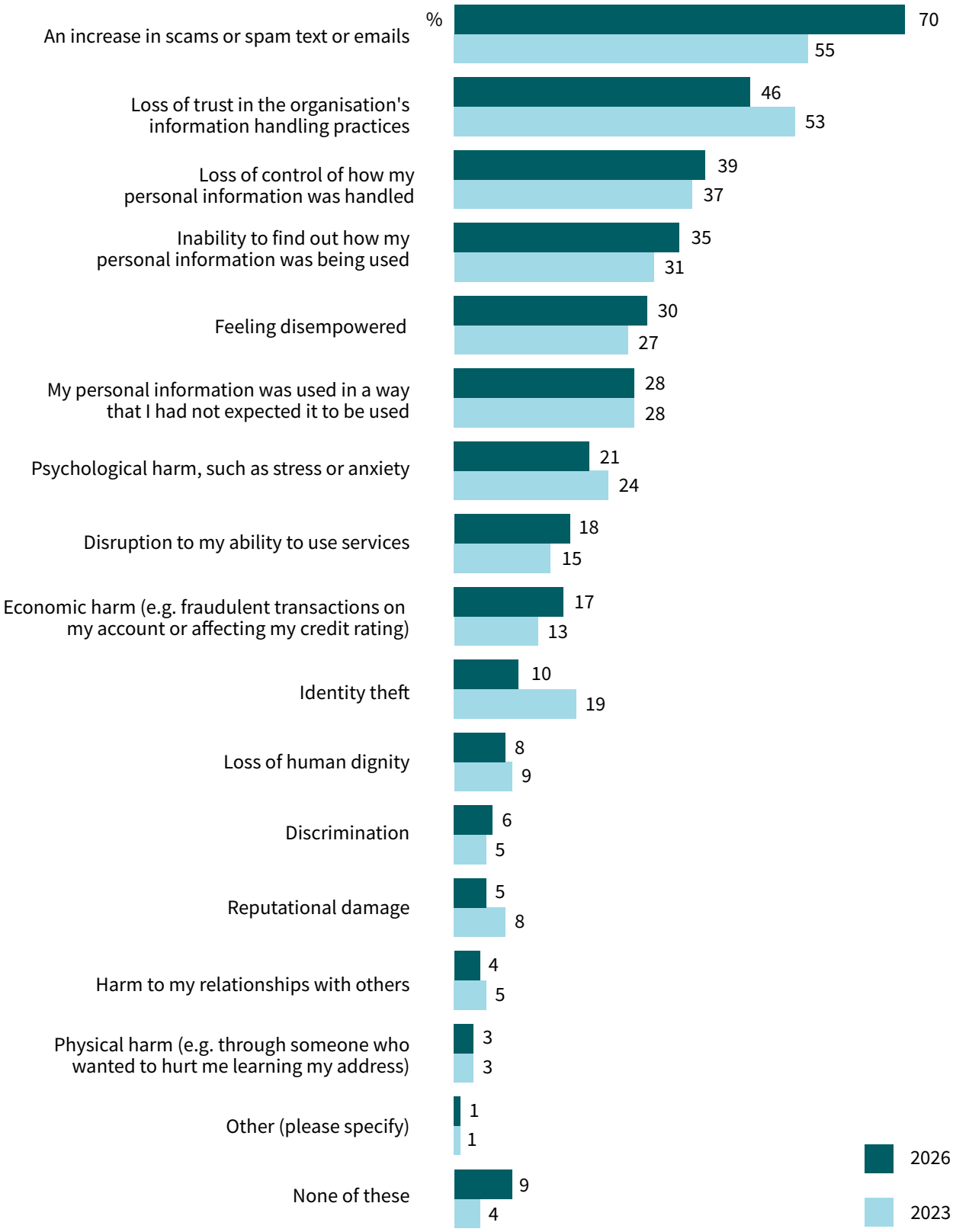
- loss of trust in the organisation's information handling (46%, down from 53% in 2023)
- loss of control over their personal information (39%)
- unable to find out how data is used (35%)
- feeling disempowered (30%)
- having information used in unexpected ways (28%).

This indicates that impacts of privacy breaches extend beyond nuisance contact to broader confidence in how organisations handle and explain personal information. When viewed overall, findings suggest that privacy harms can shape not only people's exposure to risk (such as scams and spam), but also their expectations of organisational accountability and willingness to engage.

Experiences of harm from privacy breaches vary by age, which may reflect different exposure points and expectations about acceptable data handling.

- Australians aged 25+ are more likely than those aged 18–24 to report increased scams or spam (72% vs 54%).
- Those aged 18–64 are more likely than those aged 65+ to report loss of trust in organisations (49% vs 33%).
- Younger Australians aged 18–24 are also more likely to report their personal information being used in unexpected ways (46% vs 26% of those aged 25+), suggesting that 'unexpected use' may be a particularly important driver of concern for younger people.

Figure 22 Personal experiences resulting from poor handling of personal information by organisations



Bar chart segments follow the same top-to-bottom order as the legend

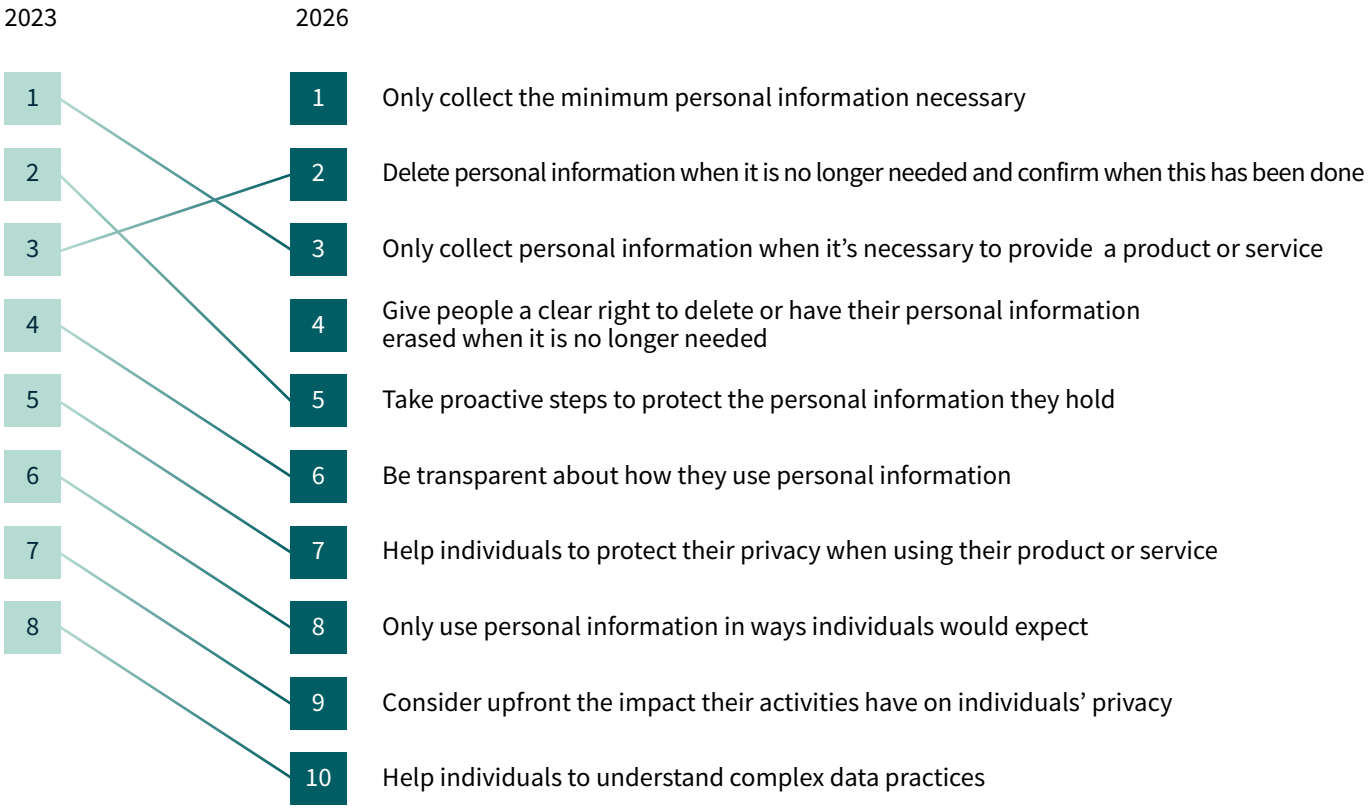
P6. Which of the following have you experienced because of a problem with how your personal information was handled by an organisation?
Base: All Australians aged 18+. (2026: n=1,099, 2023: n=540)
Notes: Don't know (0%) and refused (<0.5% in 2026) not displayed.

Ways for organisations to protect personal information

Australians place greatest importance on limiting data collection and ensuring timely deletion as key ways organisations should protect personal information. The top 3 priorities are collecting only the minimum necessary information, deleting data when no longer needed, and only collecting what is required to provide a service.

Compared to 2023, there is reduced emphasis on several measures, including necessary data collection, proactive protection, transparency, helping individuals protect their privacy, and using information in expected ways.

Figure 23 Most important ways organisations can protect personal information



P8. There are many ways an organisation can protect your personal information, which of these do you think is the most important?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,626)

Responsibility for privacy risk prevention and data breaches

Australians overwhelmingly place responsibility for data breaches on organisations that collect and hold personal information.

- Nine in 10 (91%, up from 87% in 2023) say **organisations** are responsible.
- Over half (56%) say **third-party providers or contractors** are responsible.
- Almost 3 in 10 (29%, up from 15% in 2023) say **government or regulators** are responsible.
- Very few (3%) believe **individuals** are responsible.

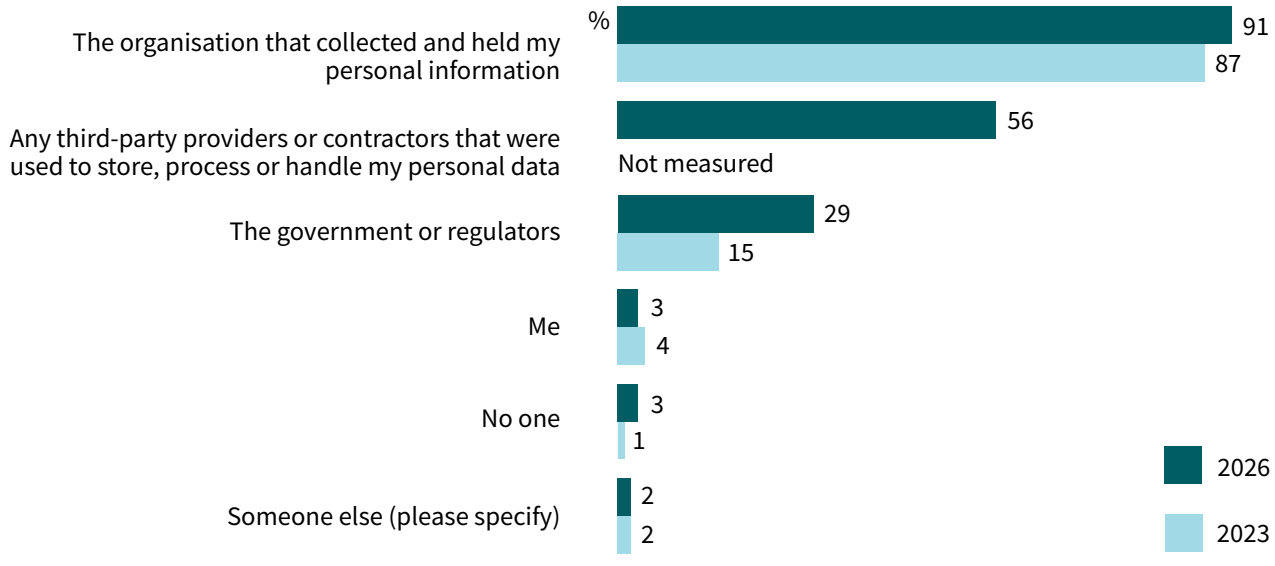
This suggests strong community expectations that accountability should sit primarily with entities that control data collection and custody, with a growing expectation that oversight bodies also have a role when breaches occur. This is an expectation that can shape trust in organisations' capacity to manage risk and respond effectively.

Views on responsibility vary across groups and levels of breach awareness.

- Older Australians aged 50+ are more likely to say organisations are responsible (95% vs 89% of those aged 18–49).
- Those who speak a language other than English are more likely to say government or regulators are responsible (39% vs 26% of English-only speakers).

Awareness of data breaches also influences views on responsibility, with those aware of breaches in the past 12 months prior to the survey more likely to hold both organisations (94% vs 86%) and third-party providers (60% vs 46%) responsible, than those not aware. This pattern reflects a heightened sensitivity to shared accountability across the 'data handling chain' among those with greater exposure to breach information, reinforcing expectations for clearer lines of responsibility beyond the individual.

Figure 24 Responsibility for a data breach affecting personal information



Bar chart segments follow the same top-to-bottom order as the legend

P16. If an organisation that you used was affected by a data breach and your information was affected, who do you think should be held responsible?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,626)
Notes: Don't know (1% in 2026, 5% in 2023) and refused (<0.5% in 2026) not displayed.

Australians consistently place primary responsibility for minimising privacy risks to organisations that collect, use or share personal information, even when no immediate harm has occurred. Nearly all respondents (98%) say organisations should be responsible, with a substantial majority viewing this responsibility as very strong (86%).

This expectation is more pronounced among:

- older Australians aged 50+ (92% vs 82% of those aged 18–49)
- those aware of data breaches in the past 12 months prior to the survey (90% vs 77% of those unaware)
- English-only speakers (88% vs 81% of those who speak another language at home).

These patterns suggest broadly held norms of organisational accountability, alongside variation that may reflect differences in perceived exposure, familiarity with privacy risks, or expectations about institutional responsibility.

Similarly, organisations are primarily seen as responsible for managing privacy risks, particularly in relation to prevention, while responsibility appears more shared when it comes to responding once problems arise. Very few believe individuals should be responsible for either preventing or addressing privacy problems.

- For **preventing** privacy problems from occurring: just under half (46%) say organisations should have primary responsibility, 35% favour a shared model led by organisations, and 16% say government should be responsible.
- For **addressing** privacy problems after they have occurred: responsibility is evenly split between organisations (34%) and government or regulators (34%), with 29% preferring a shared approach led by organisations.

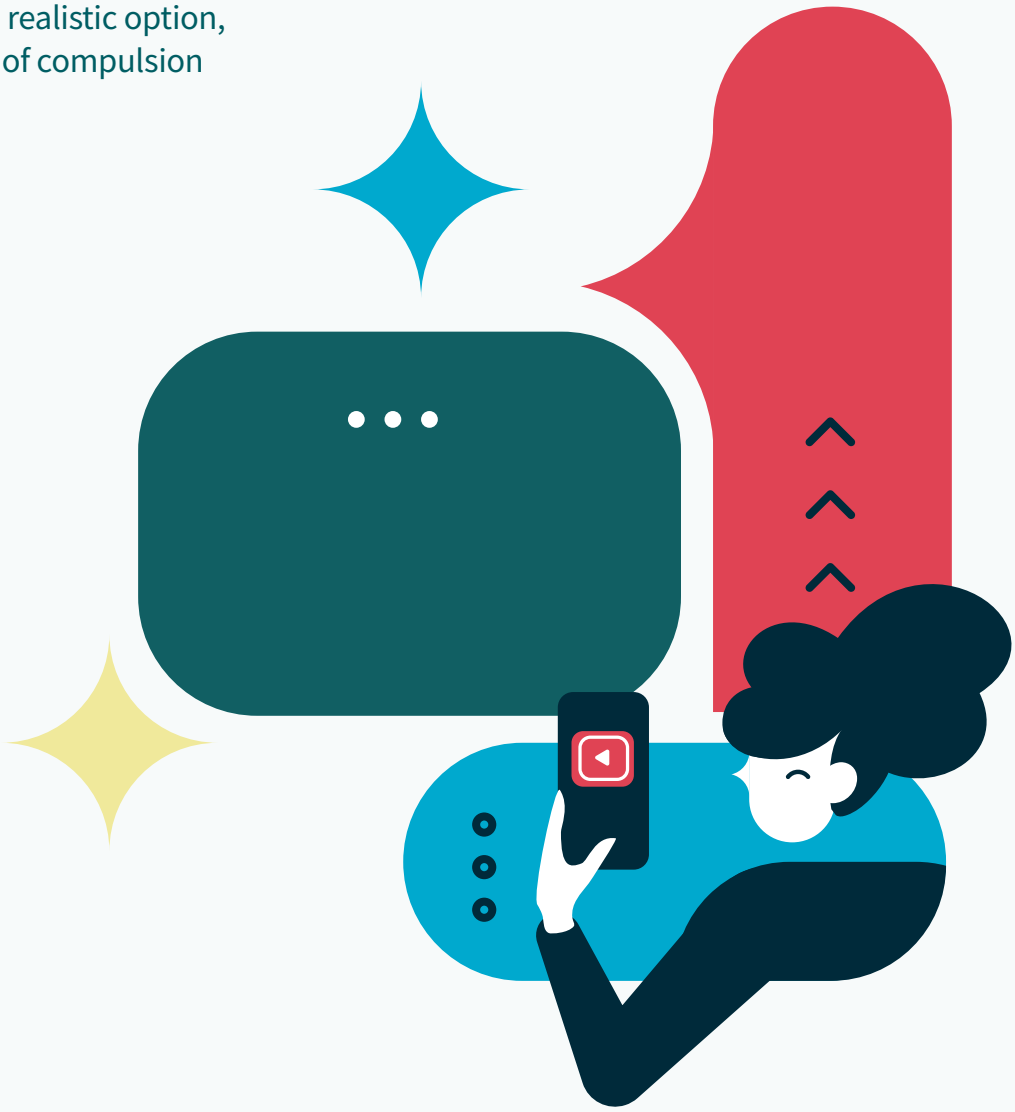
Together, these distributions suggest a distinction in how responsibilities are understood across the privacy lifecycle, with prevention more firmly associated with organisations and post-incident responses seen as requiring a broader institutional role.

Some demographic differences are evident:

- Men are more likely than women to believe organisations should carry primary responsibility for preventing privacy problems (51% vs 41%).
- Those aware of data breaches in Australia in the 12 months prior to the survey are more likely to favour a shared responsibility model led by organisations for both preventing (38% vs 28%) and addressing (32% vs 24%) privacy problems.
- Those unaware of any data breaches are more likely to believe government and regulators should take greater responsibility for prevention.

Choice and consent

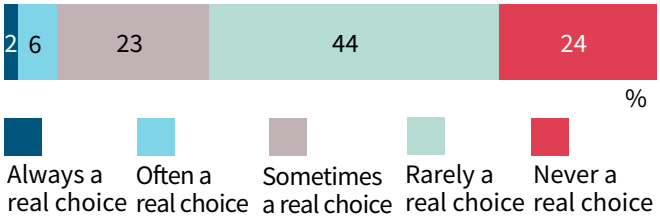
Australians generally do not perceive consent requests as meaningful choices, with many viewing them as something they must accept to use a service. Similarly, sharing personal information in everyday situations is often seen as unavoidable rather than optional, particularly when access to essential services or opportunities is at stake. These perceptions are accompanied by a strong sense of limited control over personal information and a belief that opting out is not a realistic option, reinforcing a broader feeling of compulsion rather than genuine agency.



Meaningfulness of consent

Australians generally do not feel that 'consent to use data' represents a genuine choice, with around two-thirds (68%) saying it rarely or never feels like a real choice and instead something they have to click through to continue.

Figure 25 Perceived meaningfulness of consent when organisations use personal data



Rarely/never a real choice **68**

Bar chart segments follow the same left-to-right order as the legend

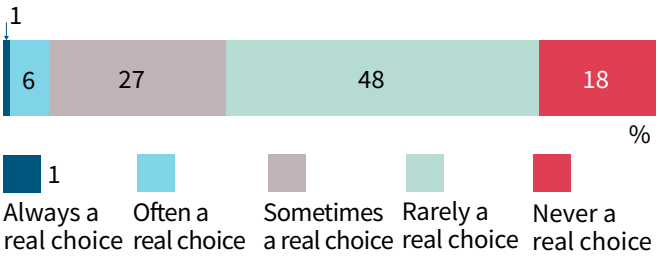
FAIR4. When organisations ask for your consent to use your data, how often does that feel like a real choice - or just something you have to click to keep going?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Perceived control over personal information

Similarly, in everyday situations, sharing personal information is also not seen as a genuine choice, with two-thirds (65%) saying it rarely or never feels like a real choice and is instead something they must accept to access services.

The feeling of rarely or having no real choice in sharing personal information is higher among those who always or often accept privacy policies without reading them (72% vs 51% of those who do so less often).

Figure 26 Perceived choice when sharing personal information in everyday situations



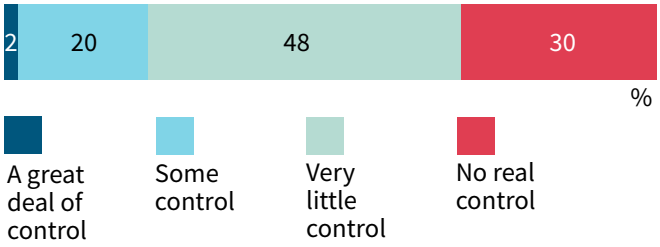
Rarely/never a real choice **65**

Bar chart segments follow the same left-to-right order as the legend

PAR4. In everyday situations, how often does sharing your personal information feel like something you can genuinely choose, rather than something you have to accept to use a service?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Reflecting this perceived lack of choice, most Australians feel they have limited control over their data, with over three-quarters (78%) reporting very little or no real control over how their personal information is collected and used, including managing privacy settings, opt-outs, or deletion.

Figure 27 Perceived level of control over how personal information is collected and used



Very little/no real control **78**

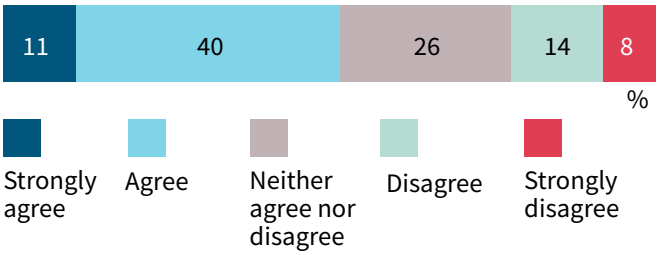
Bar chart segments follow the same left-to-right order as the legend

PAR2. How much real control do you feel you have over how your personal information is collected and used (for example, through privacy settings, opt outs, or ways to delete your personal information)?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Acceptance of data sharing to avoid service exclusion

As a result, many Australians feel compelled to share personal information, with over half (52%) agreeing they do so because not sharing would mean missing out on essential services or opportunities, particularly among those aged 25–49 compared to older Australians aged 50+ (58% vs 46%).

Figure 28 Accepting personal information sharing is a condition to accessing essential services or opportunities



Strongly agree/Agree **52**

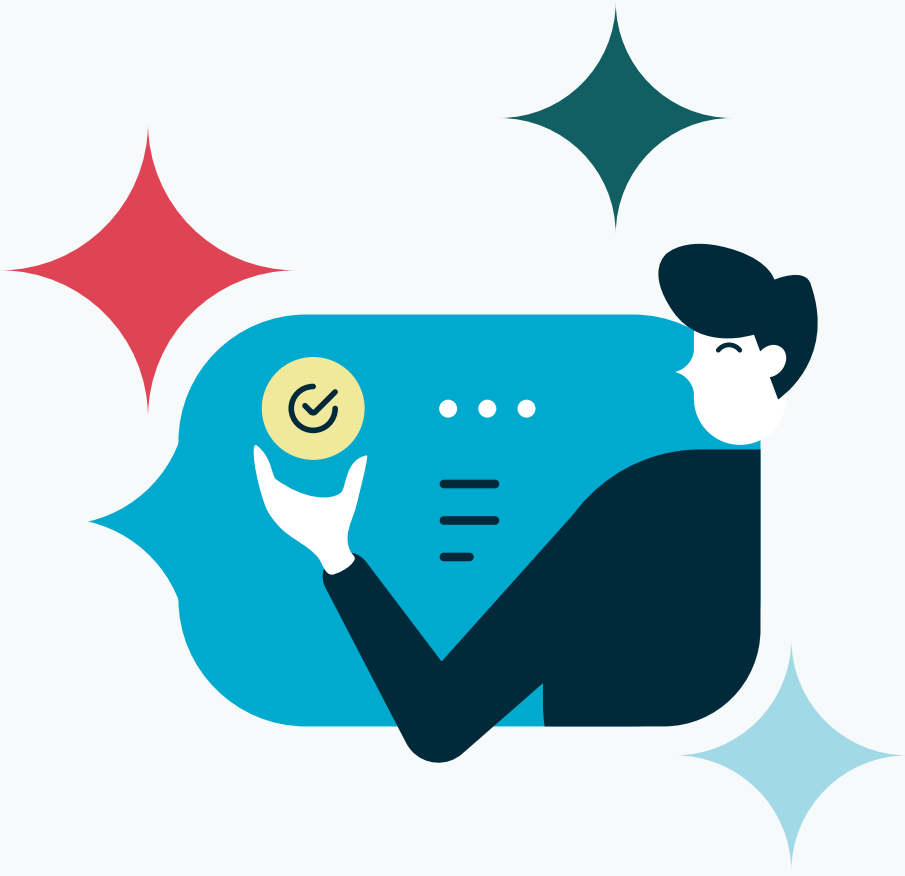
Bar chart segments follow the same left-to-right order as the legend

PAR3. To what extent do you agree or disagree with the following? a) I accept sharing personal information because not sharing personal information would mean missing out on essential services or opportunities.
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Data collection and practices

Australians increasingly view current data practices as inconsistent and often unfair, particularly where there is a lack of transparency, limited control, and little genuine choice. While data collection is seen as acceptable under clear conditions such as purpose limitation, consent, and data minimisation, there is strong opposition to practices involving sensitive information, vulnerable groups, or commercial exploitation. Overall, perceptions of fairness are closely tied to trust, control, and proportionality, with many feeling that organisations hold too much power and that risks are not justified by the benefits.

At the same time, Australians believe there should be clear limits on what personal information can be collected, especially for sensitive and intrusive data, and express growing concern about practices such as overseas data transfers.



Perceived fairness of data practices

Australians tend to view organisations' current data practices as uneven and frequently falling short of expectations. Over half say practices are sometimes fair and sometimes unfair (53%), while more than one third view them as mostly or always unfair (35%), highlighting ambivalence rather than broad confidence in how personal information is handled in practice.

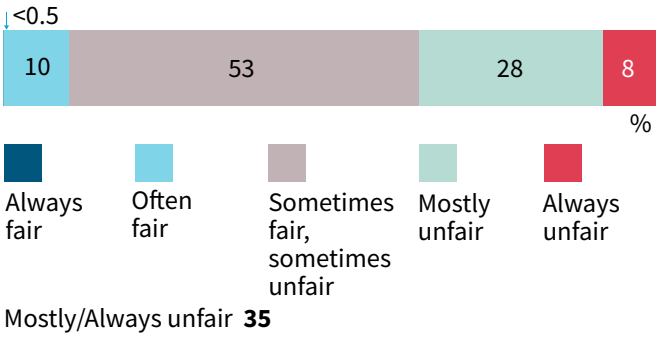
Perceptions vary by gender, with men more likely than women to judge organisations' day-to-day data practices as mostly or always unfair (40% vs 30%), while women are more inclined to characterise these practices as inconsistent (59% vs 49%).

Prior concerns also appear to shape views. Those who have had concerns about how organisations handle their data are twice as likely to perceive data practices as unfair (43% vs 21% of those without concerns). This perspective aligns with lower reported agency among this group, including:

- feeling that consent is rarely or never a real choice (46% vs 13% of those who feel consent is at least sometimes a real choice)
- the perception of little or no control over their data (41% vs 15% of those with some or a great deal of control)
- the belief that sharing personal information is rarely or never a genuine choice (46% vs 14% of those who feel it is at least sometimes a choice).

These associations suggest that perceptions of unfairness tend to cooccur with broader feelings of constrained choice and limited control over personal information.

Figure 29 Perceived fairness of organisations' real-life data practices



Mostly/Always unfair **35**

Bar chart segments follow the same left-to-right order as the legend

FAIR1. Thinking about how organisations collect, use and share personal information in Australia today, how often do you feel these data practices are fair in real life, rather than just on paper (e.g. in privacy policy or terms and conditions)?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

When data collection feels acceptable

About 9 in 10 (92%) Australians find data collection acceptable under certain conditions. Australians are more likely to accept data collection when:

- the purpose is clear and specific (69%)
- they can opt in or consent (68%)
- when only the minimum necessary information is collected (66%)
- they can opt out of non-essential collection (61%).

Safeguards and trust also play a role, though are less prominent, including limits on how long data is kept (52%) and trust in the organisation (44%).

Figure 30 Situations in which collecting personal information feel acceptable

FAIR2. In which situations do collecting personal information feel acceptable to you?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Australians typically view practices that involve sensitive data, vulnerable groups, or commercial exploitation as unfair or unreasonable.

Compared to 2023, there has been a slight increase in the proportion who view these practices as unfair or unreasonable across most use cases, except for online tracking, profiling, and targeted advertising to adults using personal but not sensitive information (e.g. work history, age, interests), which is seen as more fair and reasonable in 2026 (30%, up from 24% in 2023).

Strong opposition remains for other practices involving greater risk or harm. More than 9 in 10 Australians consider the below activities to be unfair or unreasonable:

- **Sale or trading of personal information** (96%, up from 87% in 2023).
- **Online tracking, profiling and targeted advertising** to children (96%, up from 89% in 2023) or vulnerable individuals (e.g. gambling companies targeting gamblers) (95%, up from 88% in 2023).
- **Location tracking where not required** for a location-based service (94%, up from 87% in 2023).
- **Training AI models and products** such as chatbots (93%).
- **Data scraping** from online platforms (e.g. collecting photos of people from social media platforms without their knowledge) (92%, up from 81% in 2023).
- **Differential pricing** (e.g. different people being shown different prices based on their browsing history, location, device type or past purchases) (91%).
- **AI-informed decision-making** that has a significant effect on an individual (e.g. for hiring decisions or to assess eligibility for a loan) (91%, up from 70% in 2023).
- **Targeted advertising** based on **sensitive information** (e.g. health information, racial or ethnic origin) (91%, up from 84% in 2023).

Drivers of perceived unfairness

Australians are most likely to perceive data handling as unfair when there is a lack of transparency and excessive collection. The top concerns are:

- not knowing how information will be used or shared (81%)
- not knowing how or where it is stored (76%)
- excessive data collection, including when the a mount collected is not proportionate (70%) or could be reduced (67%).

Many also see data handling as unfair when they do not have meaningful choice or control, including when:

- they cannot refuse or limit practices (66%)
- they feel the organisation has power over them (61%)
- the risks of data use are not justified by the benefits (59%).

Limits on what data should not be collected

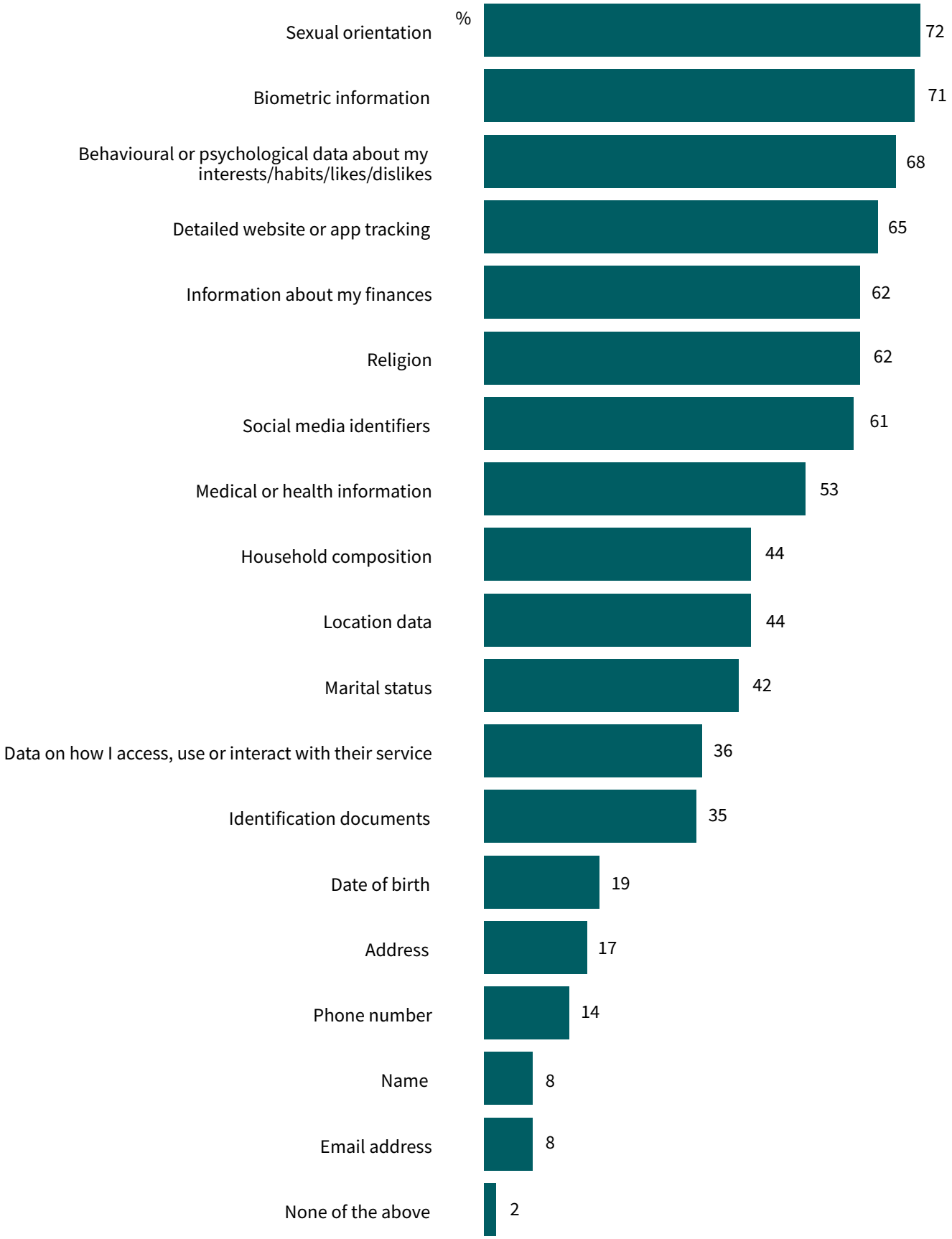
Australians strongly believe that there are limits to what personal information organisations should collect, regardless of the purpose, with over 9 in 10 (92%) holding this view. This sentiment is more pronounced among older Australians aged 50+ (95% vs 89% of those aged 18–49).

Views about what constitutes excessive or unjustified data collection vary strongly by the sensitivity of the information. Australians are most likely to view the collection of sensitive and intrusive information as excessive or unjustified in most situations, regardless of the organisation or purpose, including data such as sexual orientation (72%), biometric information (71%), behavioural or psychological data (68%), and detailed online tracking (65%), as well as financial information and religion (both 62%).

By contrast, more basic identifying information is less likely to be seen as excessive, with relatively few viewing details such as date of birth (19%), address (17%), phone number (14%), name (8%), or email address (8%) as unjustified to collect.

Older Australians aged 50+ are more likely than younger Australians to view the collection of most types of personal information as excessive or unjustified, regardless of the organisation or purpose.

Figure 31 Types of personal information collection that feel excessive or unjustified in most situations



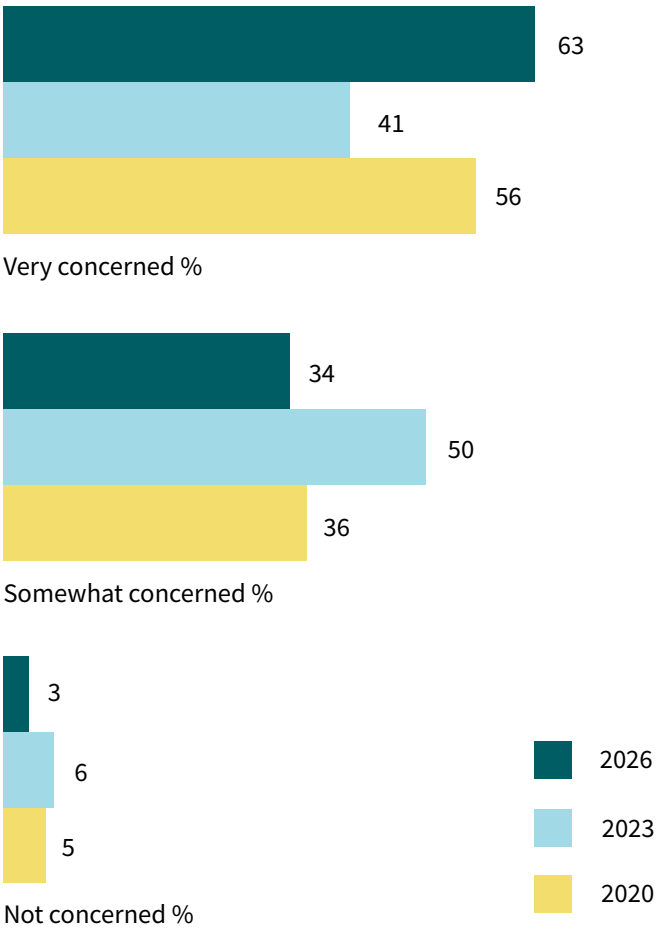
COL2. Which types of personal information collection feel excessive or unjustified to you in most situations, regardless of the organisation or purpose? Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (1%) and refused (<0.5%) not displayed.

Concerns about overseas data transfers

Concern about organisations sending personal information overseas has increased since 2023, with nearly all Australians now expressing some level of concern (97% vs 91% in 2023), including a larger share who are very concerned (63% vs 41%).

Concern is higher among older Australians aged 65+ (82% very concerned vs 58% of those aged 18–64), while younger Australians aged 18–34 are more likely to be somewhat rather than very concerned (45% vs 29% of those aged 35+), though concern remains widespread across all age groups.

Figure 32 Concern about organisations sending personal information overseas



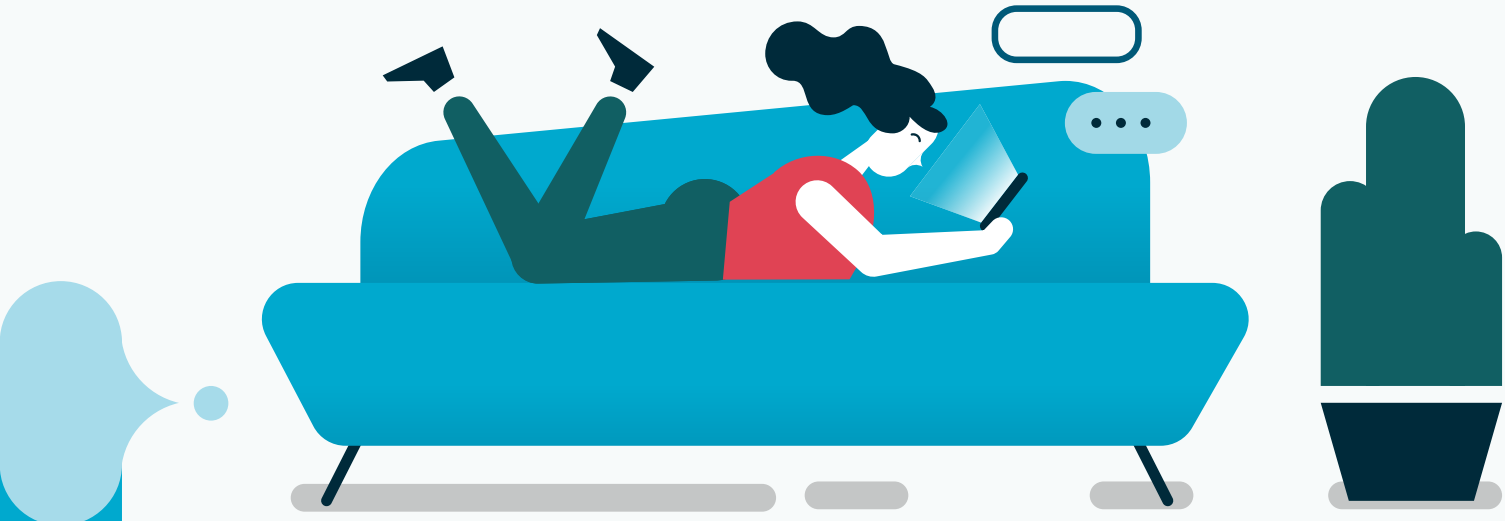
Bar chart segments follow the same top-to-bottom order as the legend

F4. Now thinking more broadly again, how concerned are you about organisations sending their customers' personal information from Australia to overseas?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,642, 2020: n=1,505)
Notes: Don't know (0% in 2026, 3% in 2023, 2% in 2020) and refused (0%) not displayed.

Digital technologies

Australians remain cautious about the use of AI, particularly where it involves personal information or impacts important decisions. There is a strong expectation that clear safeguards, transparency and human oversight should be in place, and growing demand for accountability in how AI systems operate. Acceptance of AI varies by use case, with greater comfort for lower-risk applications and clear resistance to high-stakes or automated decision-making. Australians are also generally opposed to the reuse of personal information for AI training beyond its original purpose, and expect higher standards of responsibility from trusted sectors such as government, health and financial institutions.

Similarly, Australians are increasingly cautious about biometric technologies, with discomfort outweighing comfort across most uses, especially for more advanced or predictive applications such as analysing behaviour or emotions. Acceptance depends heavily on context, with greater comfort in situations that offer clear personal or public benefit, such as identity verification, government services, and personal device use, and much lower comfort in commercial or marketing contexts. Public safety and harm prevention uses are viewed more favourably, particularly among older Australians, while trust is notably higher in government and law enforcement agencies and low in businesses, reinforcing concerns about commercial use of biometric data.



Artificial intelligence

Conditions required for acceptable AI use

Australians remain cautious about the use of artificial intelligence (AI) in decision-making that may affect them, with nearly all (96%) saying some conditions should be in place before it is used, consistent with 2023 (96%).

Transparency

Australians expect organisations to be open about how AI is used and how decisions are made, including:

- being informed when AI is being used (79%, up from 71% in 2023)
- being informed if personal information will be shared with a third-party AI provider (74%)
- clear explanations of how AI decisions are made (63%, up from 59%).

Human oversight, accountability and contestability

Australians expect AI systems to be validated and monitored, and they want people to be able to question and challenge AI-driven decisions, including:

- the right to have a human review decisions (81%, up from 73% in 2023)
- validation of AI accuracy (70%, up from 56%)
- testing for bias and discrimination (68%, up from 57%)
- the ability to challenge decisions made by AI (72%, up from 64%).

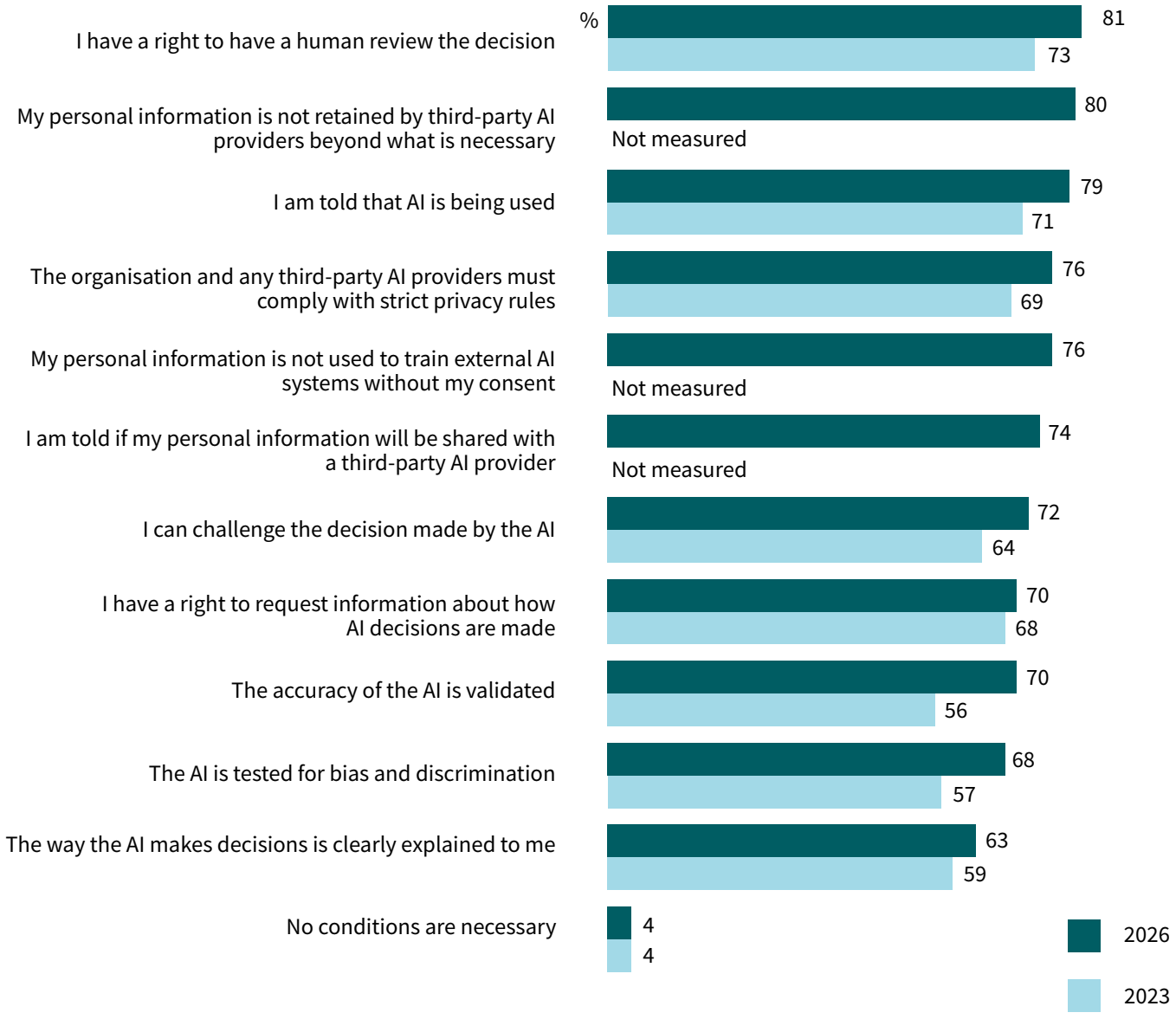
Privacy and data protection

Australians expect stronger protections for personal information used by AI, including:

- limits that personal information is not retained by third-party AI providers beyond what is necessary (80%)
- strict privacy rules for organisations and third-party AI providers (76%, up from 69%)
- personal information not used to train external AI systems without consent (76%)
- the right to request information about how AI decisions are made (70%).

Support for additional conditions is more pronounced among Australians aged 55 and over, those who speak only English at home, and those generally in the middle when it comes to adopting new technologies.

Figure 33 Essential conditions for organisations using AI to make decisions



Bar chart segments follow the same top-to-bottom order as the legend

F11. What conditions do you consider to be essential before an organisation uses artificial intelligence (AI) to make a decision that might affect you?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,642)
Notes: Don't know (1%) and refused (<0.5%) not displayed.

Acceptability of AI uses involving personal information

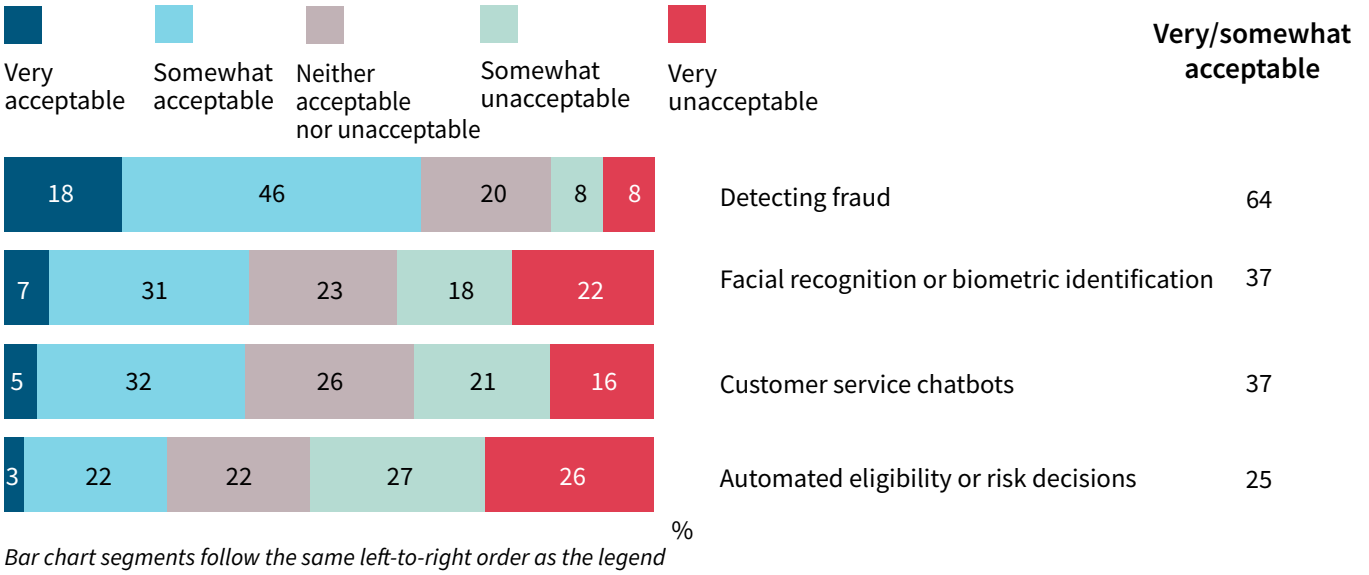
Acceptance of AI uses involving personal information varies considerably by application, with higher support for lower-risk or protective uses and greater resistance to high-stakes decision-making.

AI use for fraud detection is more widely accepted (64%), though views are more mixed for facial recognition or biometric identification (37%) and customer service chatbots (37%). Acceptance is lowest for automated eligibility or risk-based decisions, such as loan approvals or benefit eligibility, with only one-quarter (25%) viewing this as acceptable.

Acceptance of AI uses is clearly uneven across the population and reflect differing assessments of risk, familiarity and appropriateness across applications and groups:

- Younger Australians aged 18–24 are more than twice as likely as those aged 25+ to consider the use of AI for fraud detection somewhat or very unacceptable (32% vs 14%).
- Older Australians aged 50+ (49% vs 27% of those aged 18–49) and those who are typically slower to adopt new technologies (46% vs 33% of those who are earlier or mid adopters) are more likely to feel uncomfortable with customer service chatbots.

Figure 34 Acceptability of using AI with personal information for different purposes



Bar chart segments follow the same left-to-right order as the legend

F14. How acceptable do you find the use of AI for the following purposes when it involves using people's personal information?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (all <1%) and refused (all <0.5%) not displayed.

Use of personal information to train AI systems

Around 7 in 10 Australians (71%) consider it somewhat or very unacceptable for organisations to use personal information originally provided for a service to train AI systems after that service has been completed, with 45% considering it very unacceptable. This aligns with broader views on fairness, with 93% of Australians considering the use of personal information to train AI models and products unfair and unreasonable.

Those who consider it unacceptable for organisations to use personal information to train AI systems after a service has been completed are more likely to be:

- older Australians aged 65+ (81% vs 68% of those aged 18–64)
- English-only speakers (75% vs 59% of those who speak a language other than English at home).

Expectations of responsible AI use by sector

Trust and perceived obligations around AI governance vary clearly by sector, organisational role and context, with higher expectations placed on public and essential service organisations.

Australians are most likely to expect responsible AI use from:

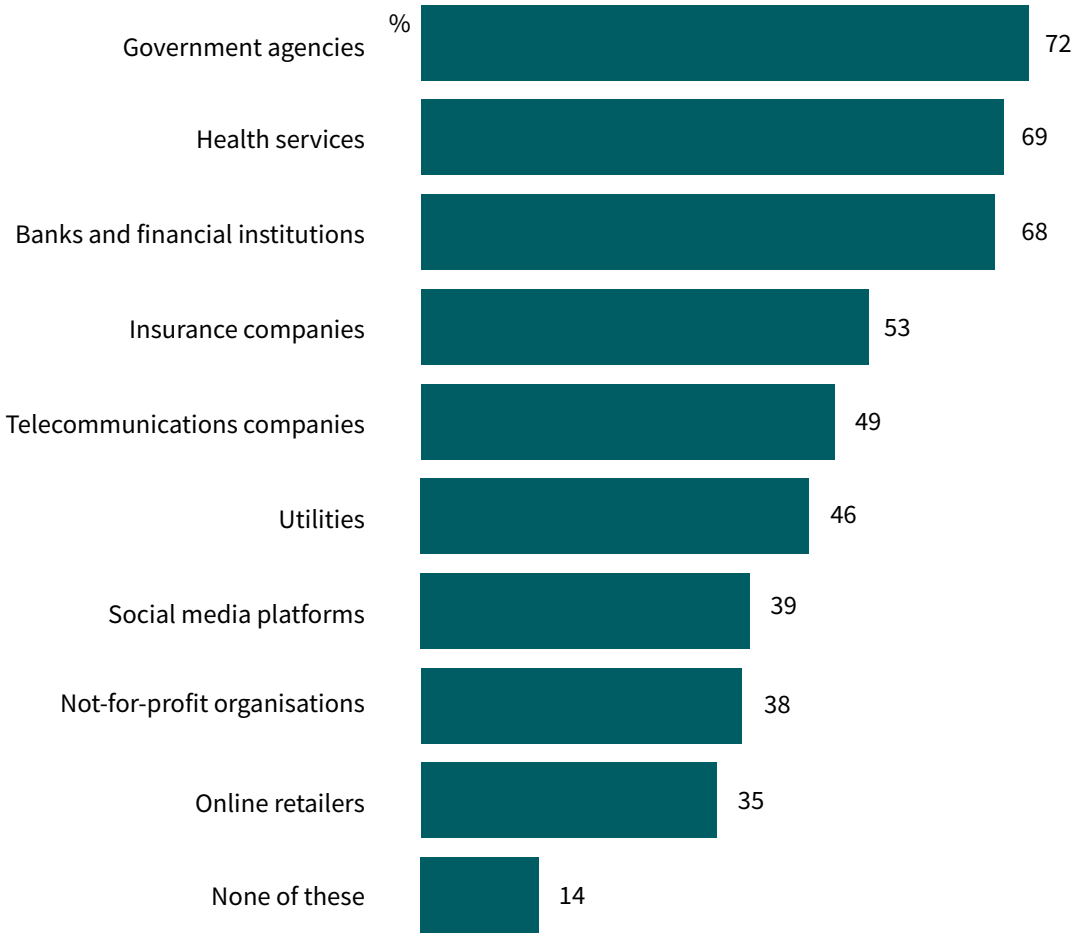
- government agencies (72%)
- health services (69%)
- banks and financial institutions (68%).

In contrast, expectations are notably lower for sectors with more commercial or platform-based models, including:

- social media platforms (39%)
- not-for-profit organisations (38%)
- online retailers (35%).

Women are more likely than men to expect responsible AI use from government agencies (75% vs 69%), health services (74% vs 64%), insurance companies (56% vs 49%), and telecommunications companies (54% vs 45%). Older Australians aged 50+ are also more likely than those aged 18–49 to expect responsible AI use across most sectors, with the exception of social media platforms, where expectations do not differ by age.

Figure 35 Expected responsible use of AI by organisation type



F16. From which types of organisations do you expect more responsible use of AI with your personal information?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (0%) and refused (0%) not displayed.

Biometric technology

Biometric analysis uses a wide variety of techniques, such as artificial intelligence, to make assumptions or predictions about the characteristics of an individual from their biometric data.

Comfort with biometric analysis

Comfort with the use of biometric analysis remains generally low, with Australians more likely to report discomfort than comfort across most applications. Comparisons over time suggest that unease may be increasing, with higher levels of discomfort reported across several use cases over the past 3 years since the previous iteration in 2023.

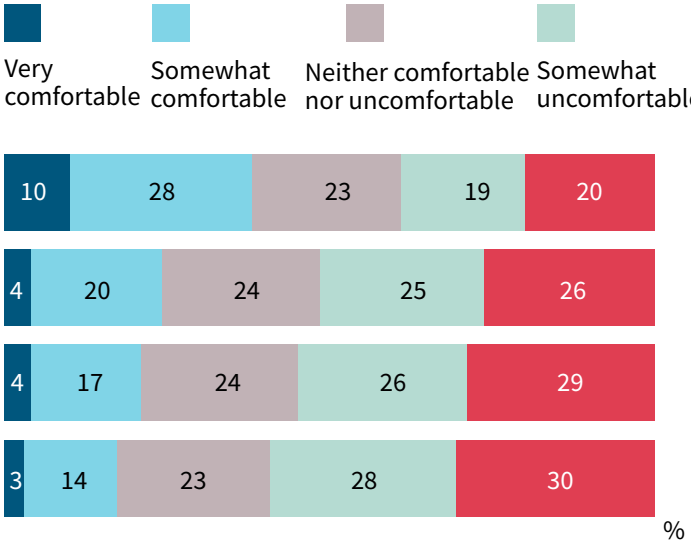
Views are most evenly divided when biometric analysis is used to determine health or disease status, with similar proportions feeling comfortable (38%) and uncomfortable (39%), although comfort has declined since 2023 (45%).

For all other applications, discomfort clearly outweighs comfort. Compared with 2023, a larger share of Australians report feeling uncomfortable with the use of biometrics for more interpretive or inferential purposes:

- estimate attributes such as age, sex, gender or ethnicity (51% vs 38%)
- identify behaviours or predict actions (55% vs 44%)
- assess emotions (58% vs 51%).

Attitudes towards biometric analysis also vary by familiarity with emerging technologies and technology adoption. Those who identify as earlier adopters of new technology are more likely than those slower to adopt to feel comfortable with biometric analysis to estimate attributes such as age, sex, gender or ethnicity (36% vs 22%) and to determine a person's health or disease status (50% vs 35%).

Figure 36 Comfort with the use of biometric analysis for different purposes



Bar chart segments follow the same left-to-right order as the legend

	Very/somewhat comfortable	
	2023	2026
To determine the health or disease status of a person	45	38
To estimate the age, sex, gender or ethnicity of a person	36	25
To identify the behaviours of a person that may indicate the likelihood of them doing certain things	29	21
To identify how a person is feeling or their emotional state	27	18

B1. How comfortable are you with the use of biometric analysis for the following?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653)
Notes: Don't know (0%) and refused (0%) not displayed.

Comfort with one-to-one uses of biometric information

Comfort with the use of biometric information, where a person's biometric data is matched against their own stored record to verify their identity, varies by context, with higher comfort in security-sensitive or personal-use scenarios and lower comfort in commercial or discretionary settings.

Australians are more likely to feel comfortable using biometric information for:

- passport control at airports (65%)
- personal devices such as unlocking a phone or collecting fitness data (61%, continuing an upward trend from 39% in 2020 and 55% in 2023)
- accessing government services (56%)
- everyday banking (55%)
- domestic flights (50%, down from 55% in 2023).

Comfort is comparatively lower in more optional or commercial contexts, reflecting greater sensitivity to the perceived necessity of biometric use in those scenarios:

- work or study settings (39%, down from 45% in 2023)
- verifying age online (33%)
- accessing business services (27%, down from 36%)
- entering entertainment venues (26%, down from 33%).

Younger Australians aged 18–34 are more likely than those aged 35+ to feel uncomfortable using biometric information to verify their age online (54% vs 37%), suggesting age-based differences in how this specific use case is received.

Comfort with one-to-many uses of biometric information

Comfort with one-to-many uses of biometric information, where a person's biometric data (such as facial recognition) is compared against many records in a database to identify who they are, varies strongly by context, with higher reported comfort in public safety and regulated harm-prevention settings and lower comfort in commercial applications.

Australians are more likely to feel comfortable with biometric information being used for:

- public safety by state and federal police (57%)
- identifying self-excluded individuals in gambling venues (50%)
- excluding patrons from licensed venues based on past behaviour (47%).

Support for these uses is stronger among older Australians, particularly those aged 50+ for police use (66% vs 50% of Australians aged 18–49), and those aged 65 and over for gambling venues (61% vs 47% of Australians aged 18–64) and licensed venues (57% vs 34%).

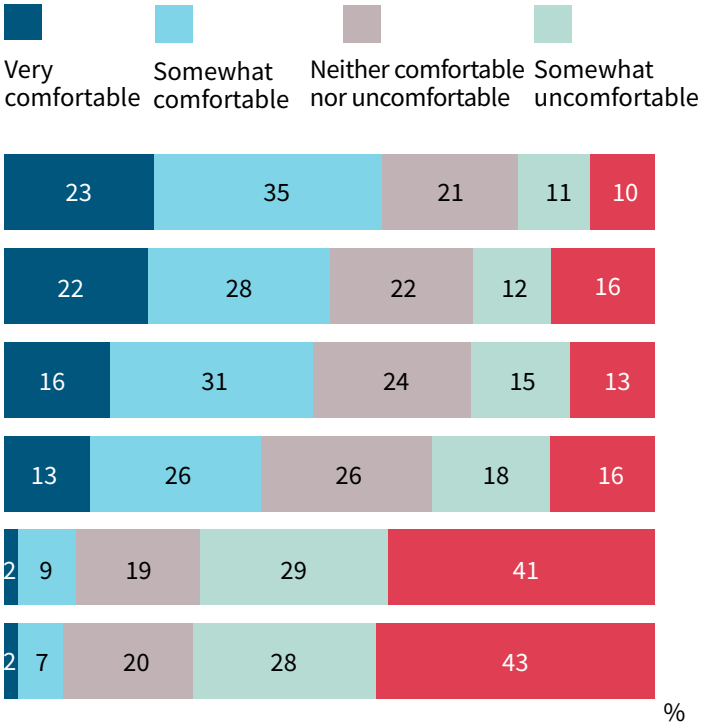
By contrast, views are more mixed when biometrics information is used by retail stores to exclude customers due to past behaviours (39% comfortable vs 35% uncomfortable).

Comfort is lowest for personalisation and advertising uses, with only one in 10 Australians comfortable with:

- retail stores recognising customers to recommend products (11%, down from 19%)
- shopping centres targeting advertisements (9%, down from 17% in 2023).

Women are more likely than men to feel uncomfortable with these uses, including retail personalisation to recommend products using biometric information (73% vs 66%) and exclusion based on past behaviour (38% vs 31%), suggesting gender-based differences in how these applications are received.

Figure 37 Comfort with one-to-many uses of biometric information



	Very/somewhat comfortable	
	2023	2026
State and federal police for public safety	60	57
Gambling venues identifying individuals who have self-excluded from gambling areas	45	50
A licenced venue excluding patrons due to past behaviour	46	47
A retail store excluding customers due to past behaviour	40	39
A retail store recognising customers in store so retail staff can recommend products	19	11
A shopping centre targeting advertisements to shoppers	17	9

Bar chart segments follow the same left-to-right order as the legend

B3. How comfortable are you with the use of your biometric information in the following situations?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653)
Notes: Don't know (0%) and refused (0%) not displayed.

Trust in organisations' handling of biometric information

Trust in organisations to collect and use biometric information varies significantly by sector, with higher trust in government-related bodies and lower trust in businesses.

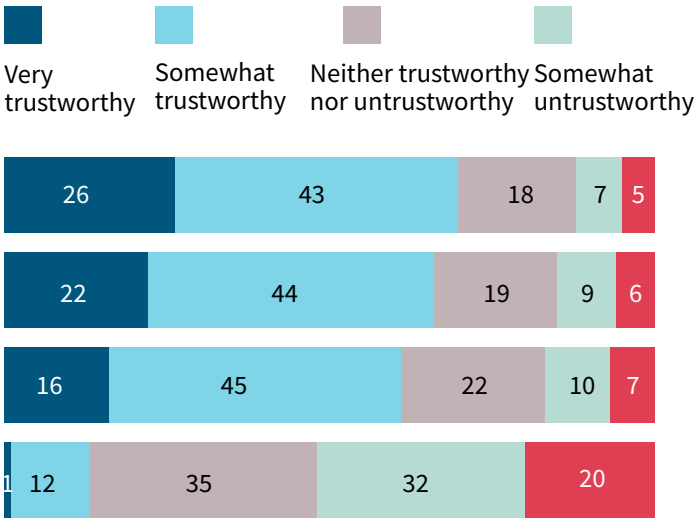
Australians are more likely to consider the following organisations trustworthy, all broadly consistent with 2023 levels:

- border security (70%)
- state and federal police (66%)
- government agencies (60%).

Older Australians aged 65+ are more likely than those aged 18–64 to rate these institutions as very trustworthy, including border security (35% vs 24%), police (33% vs 19%), and government agencies (25% vs 13%).

In contrast, trust in businesses is much lower, with one in 8 (13%) considering them trustworthy, a further decline from 24% in 2023. Men are more likely than women to view businesses as untrustworthy (56% vs 49%).

Figure 38 Trust in organisations' handling of biometric information



	Very/somewhat trustworthy		
	2020	2023	2026
Border security	N/A	69	70
State and federal police	N/A	65	66
Government agencies	48	57	60
Businesses	23	24	13

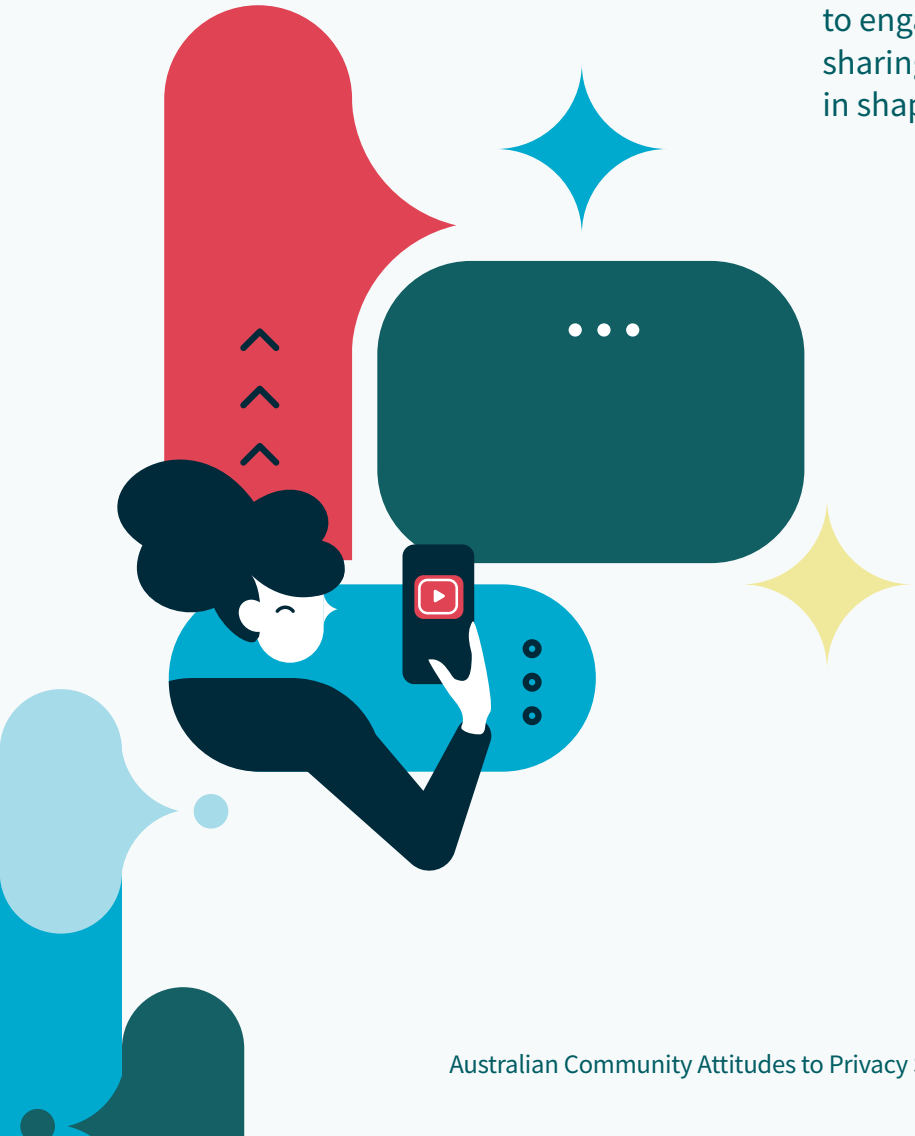
Bar chart segments follow the same left-to-right order as the legend

B4. In your opinion, how trustworthy are the following to collect and use biometric information?
Base: All Australians aged 18+. (2026: n=1,504, 2023: n=1,653)
Notes: Don't know (0%) and refused (0%) not displayed.

Privacy trade-offs and value exchange

This section explores how Australians think about the trade-offs involved in sharing personal information for convenience, and what they expect in return.

Overall, Australians are sensitive to when the balance of this exchange feels unfair, particularly when they lack choice, clarity or perceive that organisations benefit more than they do. At the same time, most believe these trade-offs could be reduced through better system and service design, rather than accepted as a necessary part of digital services. Importantly, greater confidence that personal information is handled fairly and responsibly would increase willingness to engage with services that require data sharing, highlighting the central role of trust in shaping participation.



When convenience-driven data sharing feels unfair

Australians are attuned to fairness when sharing personal information for convenience, such as saving time, efforts, or making services easier to use.

Australians are more likely to view data sharing as unfair when:

- too much personal information is collected (81%)
- there is limited ability to opt out (77%)
- the benefits mainly favour organisations rather than individuals (70%)
- the risks are not clearly explained (69%).

Those who feel that sharing personal information or providing consent is rarely or never a genuine choice are more likely to identify a broader range of situations in which such data sharing feels unfair, although the relative order of concerns is similar to that observed across the overall population.

Perceived inevitability of privacy trade-offs

Most Australians believe that privacy trade-offs in data practices (i.e. giving up personal information for convenience or services) could be reduced through better system and service design.

Around 3 in 5 (61%) say these trade-offs are often or almost always avoidable, including 22% who say they are almost always avoidable and 39% who say they are often avoidable. This is also reflected by the 52% who accept sharing personal information because they might otherwise miss out on essential services or opportunities.

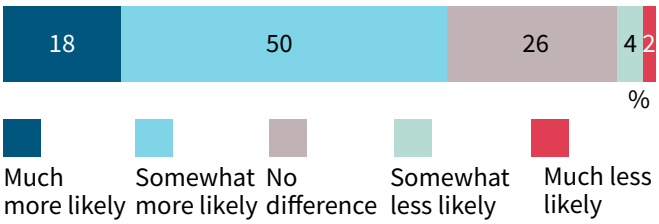
Older Australians aged 65+ (33% vs 19% of those aged 18–64) and English-only speakers (23% vs 17% of those who speak a language other than English) are more likely to believe that privacy trade-offs in data practices are almost always avoidable through better design. This view is also more common among those who feel they have very little or no control over how their personal information is collected and used, and among those who feel that consent and sharing personal information are rarely or never a genuine choice.

Impact of fair data practices on service uptake

If Australians had more confidence in how their personal information is handled, they would be more willing to use digital services or programs that require them to share it. Around two-thirds (68%) say they would be more likely to use such digital services if they felt their data was handled fairly and responsibly, while around one-quarter (26%) say it would make no difference.

Younger Australians aged 18-24 (30% vs 16% of those aged 25+) are twice as likely to say they are much more likely to use digital services if they feel more confident that their personal information will be handled fairly and responsibly.

Figure 39 Likelihood of using digital services if confident personal information is handled responsibly



Much/somewhat more likely **68**

Bar chart segments follow the same left-to-right order as the legend

TRA3. If you felt more confident that your personal information was handled fairly and responsibly, how likely would you be to use digital services or programs that require you to share personal information?
Base: All Australians aged 18+. (n=1,504)
Notes: Don't know (1%) and refused (0%) not displayed.

Vignettes: Illustrating privacy experiences

To help contextualise the findings in this report, the following vignettes present 2 hypothetical individuals whose experiences reflect common attitudes and behaviours identified in the survey. While not based on real people, each vignette draws on key data points to illustrate how Australians navigate privacy in practice.

Vignette 1: ‘Privacy-conscious and cautious’

Name: Margaret
Age: 62
Occupation: Retired nurse

Margaret has always been careful with her personal information, but over the past few years she’s found herself becoming much more vigilant. Like many Australians, she feels her concern has increased, she says that she is now “definitely more worried than 5 years ago,” something reflected by the 87% of Australians who say the same. She’s particularly uneasy about stories of data breaches and scams, which reinforce her belief that organisations don’t always handle information securely.

When Margaret interacts with services, she tries to share as little as possible. She prefers dealing with familiar providers like her GP or government services, where her trust tends to be higher. Still, even in those situations, she sometimes questions why she’s being asked for certain details. She firmly believes there should be limits, like the 92% of Australians who say there are some types of information organisations should never collect. She finds requests for things like biometric data or overly detailed personal information unnecessary in most contexts, and will often look for alternatives if something feels excessive.

Margaret is also one of the many Australians who feels that exercising privacy rights isn’t straightforward. While she supports stronger protections, including the right to deletion, which 93% of Australians back, she admits she wouldn’t always know where to start if she had a concern. Like many people, she suspects the process might be too time-consuming or wouldn’t make a difference anyway, which is why she tends to avoid lodging formal complaints. If services were more upfront and gave her meaningful control, she’d be more willing to engage, which aligns with the 68% of Australians who say they would be more likely to use digital services if they trusted how their data was handled.

For Margaret, privacy is deeply important, but managing it in practice often feels not worth the hassle.

Vignette 2: ‘Convenience-oriented and open’

Name: Daniel
Age: 29
Occupation: Digital marketing specialist

Daniel is comfortable navigating digital services and is used to sharing personal information online. He knows privacy matters, like most Australians, he agrees it’s important, but in day-to-day life, he often prioritises convenience. Signing up for apps, agreeing to privacy policies, and linking accounts feels routine, and he rarely reads the fine print, much like the 69% of Australians who say they often accept policies without reading them.

For Daniel, sharing data often feels like part of the deal. He recognises that access to services sometimes depends on it, reflecting the 52% of Australians who say they accept sharing information because otherwise they might miss out on essential services or opportunities. Still, he occasionally feels uneasy about how much control he actually has. Even though he uses tools like app permissions and account settings on his devices and accounts, he’s not always confident they make much difference, and he relates to the 78% of Australians who feel they have little or no real control over how their data is collected and used. Daniel’s views start to shift when it comes to more sensitive or behind-the-scenes data use. He’s particularly wary of things like targeted advertising based on personal data or companies using information to train AI systems after that service has been completed, both practices widely seen as unfair by Australians. While he’s open to sharing information when the benefit is clear, he expects transparency and choice.

Methodology

Overview

The Australian Community Attitudes to Privacy Survey (ACAPS) is a long-running study commissioned by the OAIC to assess Australians' awareness, understanding, behaviours and concerns around privacy. First conducted in 1990 and formalised in its current structure in 2001, the survey provides valuable time series insights into how Australians think about privacy, their experiences with the use and protection of personal information, and the actions they take to safeguard it.

ACAPS 2026 is the 7th survey in a series initiated in 2001. The methodology has evolved over the past 2 decades to reach a representative sample of Australia's population. Between 2001 and 2013, all interviews were completed via Computer Assisted Telephone Interviewing (CATI). In 2017, the methodology shifted to a hybrid online and CATI methodology, where 800 surveys were conducted via CATI and 1,000 were completed online, with respondents reached via an online research panel. In 2020, all data was collected online, with 39% of respondents recruited via telephone. In 2023, all data was again collected online, with all respondents reached via an online research panel. In 2026, data collection was primarily online, including a small proportion via CATI.

Since the previous report in 2023, Australians' attitudes toward privacy have continued to evolve in response to a rapidly changing digital environment. Ongoing high-profile data breaches and cyber incidents have sustained public concern around how organisations collect, store and safeguard personal information, reinforcing expectations for stronger accountability and transparency. At the same time, the accelerated adoption of artificial intelligence, increased use of automated decision-making, and the expansion of data-driven technologies, including biometrics and large-scale data scraping, have heightened awareness of more complex and emerging privacy risks.

The study aims to:

- provide insights on Australians' awareness, attitudes and behaviours towards privacy and understand how they have changed over time
- identify Australians' awareness of and concerns about key and emerging privacy issues
- collect data to assist the OAIC as the national privacy regulator across policy, compliance, and communications initiatives, and government agencies more broadly in policy development
- examine experiences with privacy disputes, including whether respondents have attempted to resolve a privacy-related matter with a company and their level of satisfaction with the resolution process.

Questionnaire development

The 2026 iteration of ACAPS builds on previous waves, with an increased focus on areas such as privacy complaint resolution, data minimisation, data deletion, trade-offs between convenience and value exchange, perceived control and the meaning of consent, as well as AI.

The questionnaire was jointly developed by the Social Research Centre and the OAIC.

Questionnaire development followed a staged, iterative process incorporating a co-design workshop with OAIC staff and relevant stakeholders, an exploratory qualitative research phase consisting of 6 online focus groups with general community members, and 8 cognitive testing interviews. A short validation component was also incorporated into the survey design to assess potential order effects for selected new questions.

The total survey length was 29.5 minutes (29.3 minutes online, 51.7 minutes CATI).

Sample profile

Table 1 below shows the unweighted sample distribution across key demographic profiles.

Table 1 Unweighted sample profile

Group		n	%
		1,504	**100%**
Age	18-24	126	8%
	25-34	293	19%
	35-49	379	25%
	50-64	379	25%
	65+	327	22%
Gender	Man or male	746	50%
	Woman or female	743	49%
	Non-binary	14	1%
State	NSW	487	32%
	VIC	366	24%
	QLD	285	19%
	SA	127	8%
	WA	148	10%
	TAS	49	3%
	NT	6	0.4%
	ACT	36	2%

Weighting

The sample was weighted to be representative of the Australian adult population by age, highest education level, language other than English spoken at home, number of adults in the household, geographic location (capital city/ rest of state), and state or territory of residence.

Rounding of numbers

Results are shown rounded to 2 decimal places. Due to rounding, some results in charts or tables may not add to 100%.

Fieldwork

ACAPS 2026 was conducted by the Social Research Centre between 16 and 30 March 2026, using a nationally representative sample of 1,504 Australians aged 18 years and over drawn from the Social Research Centre's probability-based panel, Life in Australia™.

Glossary and shortened terms

Glossary

Term	Definition or meaning
Artificial intelligence (AI)	Artificial intelligence was explained to respondents as follows: 'Many organisations are now using artificial intelligence (AI) or automated decision-making systems to make decisions that may affect you. In some cases, they may use AI systems developed by third-party commercial providers (e.g. ChatGPT, Grok and Gemini), which may involve sharing your personal information with those companies. These AI systems may be used to help with: • diagnosing illnesses • generating your credit score • fraud detection • making hiring decisions for employers and recruitment organisations.'
Biometrics	Biometrics were explained to respondents as follows: 'The next section is about biometrics, which is biological and behavioural information about you. This includes things like: • your fingerprints • your facial image • your voiceprint • scans of your iris or retina your DNA • the way you walk, your keystroke patterns or other physical characteristics that could be used to identify you.'
Biometric analysis	Biometric analysis uses a wide variety of techniques, such as artificial intelligence, to make assumptions or predictions about the characteristics of an individual from their biometric data.
Data breach	A data breach was defined to respondents as follows: 'A data breach is when personal information held by an organisation is accessed or disclosed without authorisation, or is lost. Data breaches may result from malicious action (e.g. cyber criminals), human error (e.g. personal information being emailed to the wrong person) or errors in business or technology processes.'
Privacy breach	The term 'privacy breach' is used to refer to a wide range of problems experienced with the handling of personal information. It is distinct from 'data breach'.

Term	Definition or meaning
Personal information	Personal information was defined to respondents as follows: 'In Australia, privacy law relates to the protection of an individual's 'personal information'. This is any information about you that identifies you or could reasonably be used to identify you. This includes things like: • your name or address • your date of birth • your financial details • photos or videos of you • your opinions and beliefs • your membership of groups and affiliations • your racial or ethnic origin • your health information • your biometrics (e.g. your facial image, DNA, fingerprints) • your sexual preferences • your criminal record.'
Organisations	Organisations is used in the survey and report as an umbrella term for private and public entities. The terms 'businesses' and 'government agencies' are used to distinguish these organisation types.
B2B	Bottom 2 box - the sum of the bottom 2 codes of a response frame.
T2B	Top 2 box - the sum of the top 2 codes of a response frame.

Shortened terms

Term	Definition or meaning
ACAPS	The Australian Community Attitudes to Privacy Survey
AI	Artificial intelligence
OAIC	Office of the Australian Information Commissioner

List of Figures and Tables

Australian Government
Office of the Australian Information Commissioner

Australian Community Attitudes to Privacy Survey 2026

oaic.gov.au/acaps
communications@oaic.gov.au

Social Research Centre

The Social Research Centre Pty Ltd
Level 5, 350 Queen Street, Melbourne VIC 3000
PO Box 13328, Law Courts VIC 8010
03 9236 8500 | info@srcentre.com.au
srcentre.com.au

OAIC