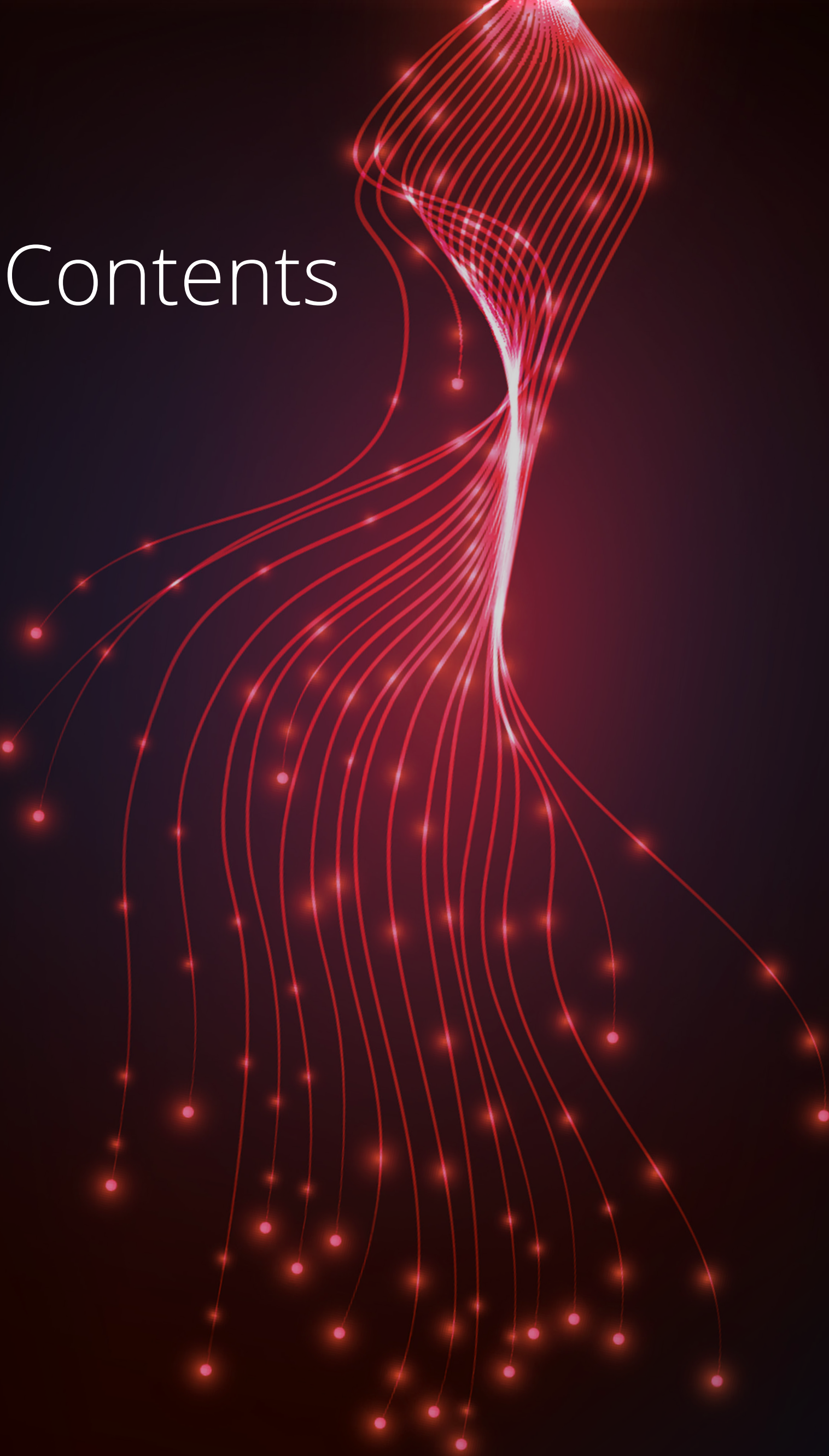




Data. Whose responsibility is it anyway?

Deloitte Australia Privacy Index 2023

An abstract graphic on the left side of the page, consisting of numerous thin, glowing red lines that originate from a single point at the top and fan out downwards, ending in small, bright red dots. The lines have a slight wavy, organic quality, resembling fiber-optic cables or a stylized tree structure.

Contents

i	Foreword	3
ii	About the report	4
iii	Australia’s privacy pulse: a snapshot of the nation	5
iv	Protecting people’s privacy: key actions for organisations	6
v	Privacy Index 2023	7
1	Chapter 1 Australia’s privacy pulse	10
2	Chapter 2 The privacy pursuit: what the public wants	15
3	Chapter 3 What now for organisations?	20

Foreword

When considering this year’s theme, there was only one contender: responsible data handling. These three words impact all Australians and have ramifications for every business, organisation and government department in the country.

Responsible data handling: treating individuals’ personal information with care and integrity, ensuring it’s collected, stored, processed and shared in a secure and transparent manner that respects individuals’ privacy and protects against unauthorised access or misuse.

And the country’s already felt the ramifications. Feelings are running high – Australians have told us they feel vulnerable and angry. Millions have been caught up in data breaches, their personal data has been compromised – personal information that’s requested, often required, in exchange for goods or services – and they want more done to protect it.

Privacy practices are under scrutiny, regulations and laws are being reviewed and, on top of this, data breaches are increasing in frequency and sophistication. Organisations, businesses and government are now having to review and revise their practices and must immediately transform to meet and exceed consumer expectations and keep pace with regulatory reform. But with so many moving parts, and so much at stake, how do they adapt to the changing landscape and align their strategies to achieve this?

In this year’s Privacy Index we examine and explore:

- Australia’s leading organisations’ privacy practices and commitments to privacy
- How Australians feel about the privacy landscape
- What actions Australians are taking in the pursuit of privacy
- What the public wants and from whom
- How organisations can meet and exceed consumer expectations.

To capture the mood of the nation and bring the consumer voice to life, we held focus group interviews to understand people’s feelings and behaviours towards data breaches, privacy and personal information.

We’ve built this year’s report around our findings from those interviews and the Consumer Sentiment Survey, along with insights and actions from Deloitte privacy and risk specialists.

As a result, our report elevates the nation’s voice, but also guides organisations and government on how to structure strategies and strengthen privacy practices to ensure responsible data handling.

The 2023 Privacy Index focuses on creating positive change for all Australians. We must all play a part in creating a safer, more responsible data landscape and this report will guide and support that change.

Responsible data handling may sound innocuous, but sizzling under the surface of those three words are the trust and expectations of millions of Australians.

This report equips organisations with the knowledge, tools and actions needed to earn Australian’s trust, meet their expectations and create a safer, more responsible privacy landscape.

About the report

The theme: responsible data handling

The 2023 edition of Privacy Index once again dives into the world of privacy and data to examine the privacy practices of leading Australian organisations. This year, we investigate responsibility around consumer data with a focus on organisations’ privacy practices and how they communicate their practices to consumers.

The 2023 Index

To assess organisations’ data handling practices, we looked at websites, privacy policies and annual reports to understand:

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

We then aggregated our findings to compare industries, added insights from our people surveys and focus groups, along with industry level breach and complaints data.¹ We used these results to score and rank the 10 industries – this became our 2023 Privacy Index.

The ten industry groups are:

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

Consumer Sentiment Survey and consumer trust rankings

We surveyed 1,000 Australian consumers aged 18-and-over – who demographically represent the Australian population – to understand how they feel about the privacy landscape in light of recent high-profile breaches, as well as about responsibility towards data and where they believe the line begins and ends.

We also asked consumers which industries they trust most to handle their personal information responsibly – see the consumer trust rankings on **page 8**.

Consumer focus groups

This year for the first time, we conducted additional qualitative research with consumer focus groups to better understand consumer sentiment. These focus groups were held in Melbourne over four sessions. Through these focus groups, we gathered in-depth insights and opinions directly from the consumers which allowed us to delve deeper into the attitudes, preferences and motivations that drive consumer behaviour.

See how your industry ranks on **page 7**.

i

ii

iii

iv

v

1

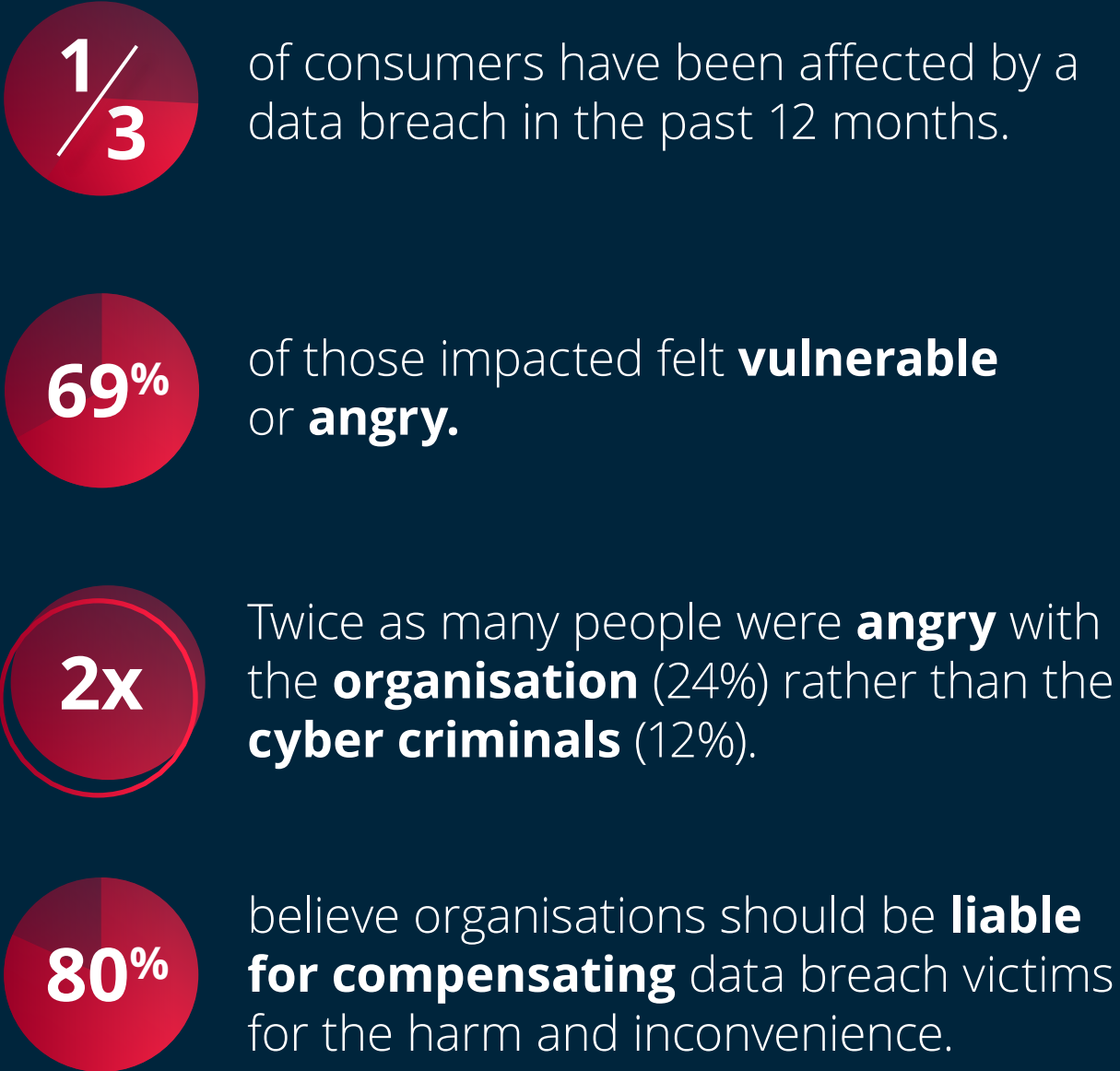
2

3

¹ Notifiable data breaches publications, Office of the Australian Information Commissioner

Australia's privacy pulse: a snapshot of how people *feel*

Into the breach: people's post-breach perceptions



The privacy pushback: taking back control



Action stations: what people want



Protecting people's privacy: *5 key actions* for organisations

The people's message is loud and clear:

Organisations must do more to protect people's personal information.



Prioritise privacy protection

Organisations should prioritise privacy and data security so they can quickly adapt to meet consumer demands.



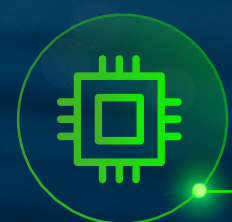
Give people agency

Savvy organisations will empower their customers to make their own choices around privacy and personal information and could even involve customers in the development of privacy policies.



Communication is key

In a world where consumers wade through complex, tedious privacy policies for key information, organisations have an opportunity to foster trust, enhance transparency and differentiate themselves by creating compelling privacy-related content that empowers and reassures customers.



Invest in technology

As data breaches increase in frequency and sophistication, conventional methods are no longer enough and new innovations and technology, such as privacy-enhancing technology (PETs) and consent management platforms (CMPs), must be explored.



Put people first

A consumer-centric approach will help future-proof organisations from upcoming regulatory reforms and enhance customer relationships.

Privacy Index 2023

How does *your industry* rank?

Industry comparison is based on analysis of how they perform in relation to the year's topic. The rankings provide a holistic view of each industry's privacy posture for the focus area of previous Index editions.

For example, the retail sector led for consent practices (as of 2020) but performed poorly in surveillance and online personalisation (as of 2022).

Responsible data handling

- 1



Information technology
- 2



Education & employment
- 3



Health & fitness
- 4



Travel & transport
- 5



Energy & utilities
- 6



Telecommunication & media
- 7



Government
- 8



Real estate
- 9



Retail
- 10



Finance

Previous rankings

	2022 Online tracking	2021 Future of privacy	2020 Consent
	6	1	3
	1	4	6
	10	7	10
	3	3	4
	8	9	7
	7	10	8
	5	2	2
	4	6	5
	9	5	1
	2	8	9

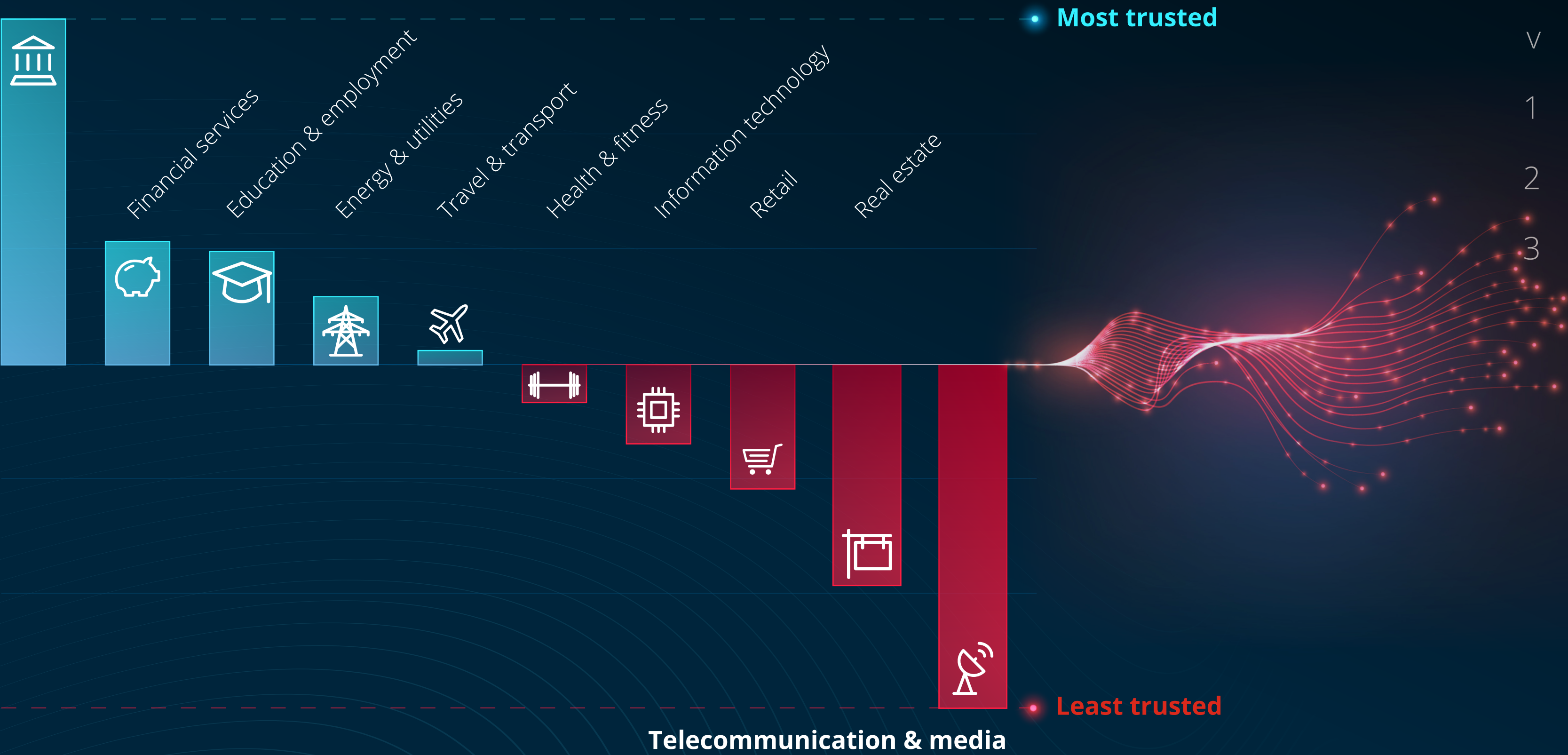
Who do consumers *trust* most with their data?

We asked consumers which industries they trust to handle their personal information responsibly.

The results were aggregated across industry sectors, giving each sector a net negative or positive trust score.

Responsible data handling consumer rankings

Government



i

ii

iii

iv

v

1

2

3

Top 2 reasons consumers trust organisations to handle their personal info responsibly:



Data security
The organisation explains clearly and transparently how they will securely store consumers' data.

90% of survey participants



Privacy policies
The organisation explains how they will maintain the consumers' privacy by displaying understandable privacy policies up-front.

87% of survey participants

Acting in the right way isn't enough, communicating privacy practices in a clear and transparent way is equally important.

Chapter 1 | Australia’s privacy pulse

We took the pulse of Australia through our survey and focus group participants to understand how Aussies feel about the privacy landscape. We explore those findings in this chapter.

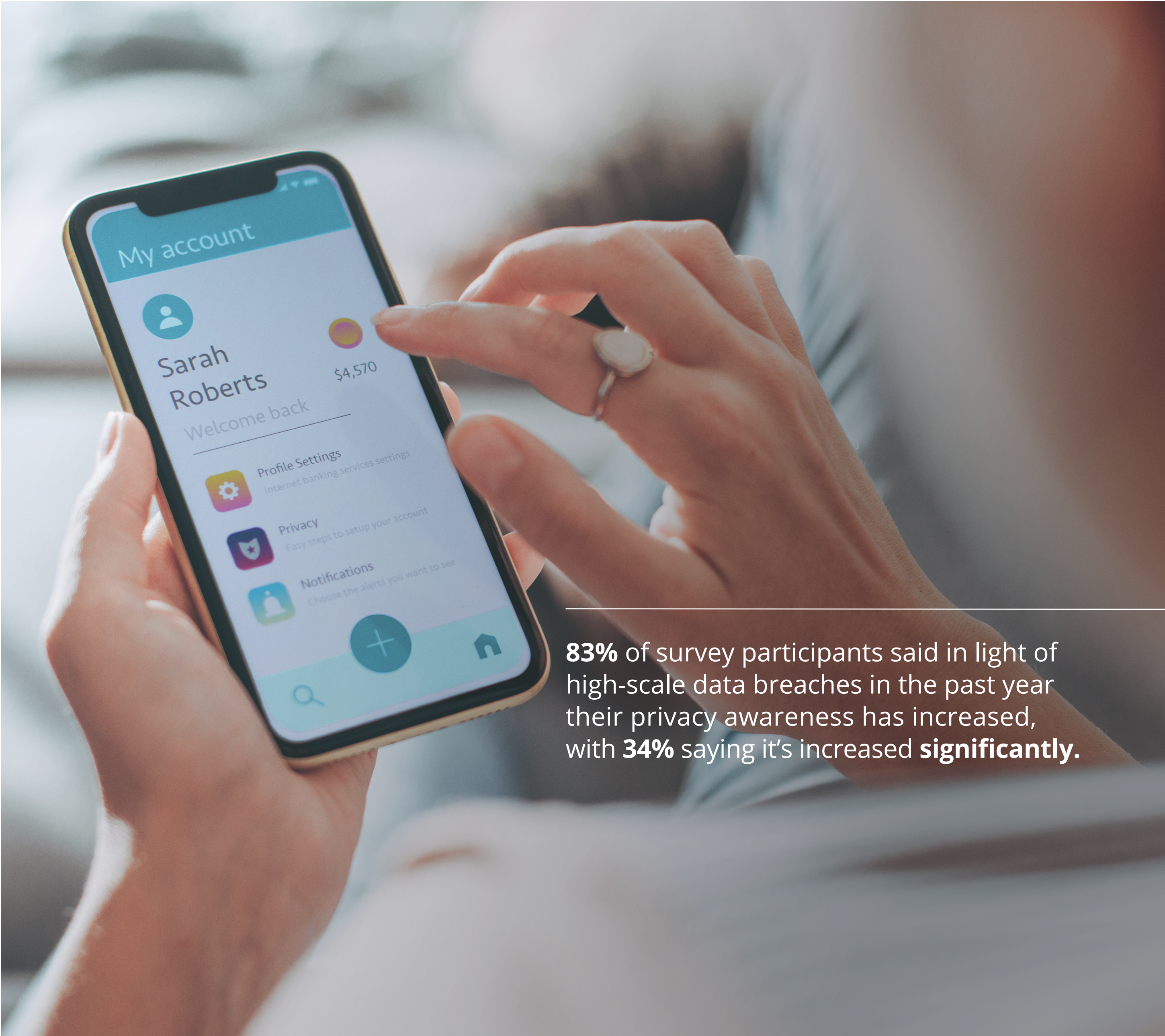
- i
- ii
- iii
- iv
- v
- 1
- 2
- 3

Every day, millions of Australians jump online to stream, browse, subscribe, login, connect, order, access, view, download, play, interact. Bills are paid, dates made, socials relayed — anywhere, anytime. Tacos, taxis, tickets are just a finger-tap away.

The world is our oyster... but not without the data exchange: name, address, phone number, bank details, DOB, place of birth, first cat's name, privacy policy skimmed, terms and conditions ticked, email verified.

Now, the world is our oyster.

Data, it's the key to contemporary living. To live, work and play today we consent to a data transaction – our personal information in exchange for service access – this quid pro quo is just part and parcel of modern life, right? But high-profile breaches and cyberattacks resulting in millions of Australians' personal details being stolen and misused have made Australia sit up and take notice.



83% of survey participants said in light of high-scale data breaches in the past year their privacy awareness has increased, with **34%** saying it's increased **significantly**.

Shaken and stirred

According to the Office of the Australian Information Commissioner (OAIC), there were 893 data breaches reported through their Notifiable Data Breach scheme in Australia last year² and as well as raising privacy awareness the breaches have shaken people's trust in organisations.

To understand how Australians feel when impacted by a breach, we asked our survey participants if they'd been affected by a data breach in the past 12 months – one-third had and 69% of those said they felt vulnerable or angry.

And it turns out that twice as many people (24%) who were impacted by a breach said they felt angry with the organisation experiencing the breach rather than the cyber criminals (12%). Anger towards the organisation was twice as likely with people aged 50-and-over (32% felt angry with the organisation) compared to those under-35 (15%).

Those feelings of angst probably explain why 80% of all survey participants believe organisations should be held liable for compensating data-breach victims individually for the potential harm and inconvenience.

But it's not just the big breaches that continue to unnerve people, there are small, intrusive daily reminders — like scam messages, phishing emails and dodgy phone calls — that we've lost control of our data.

32% of our survey respondents reported receiving multiple scam communications each week, with 17% saying they get multiple every day. Only 2% said they didn't receive any. We call this underlying, ever-present fear that we're losing the data-control battle, 'data insecurity'.

The combination of data insecurity living rent free in the country's collective psyche and frequent data breaches and scam attempts is eroding community confidence in organisations' ability to handle data responsibly. Consequently, when people are asked for personal information, they're on alert, cautious and reticent about what they share.

Does this mean we're moving from quid pro quo into an era of quid pro 'no'?

data insecurity

noun

- 1. A sense of unease and lingering worry individuals experience daily concerning the protection, control and potential risks associated with their personal information.



of consumers have been affected by a data breach in the past 12 months.



of those impacted felt **vulnerable** or **angry**.



of people believe organisations should be **held liable for compensating** data-breach victims individually.



² OAIC, Notifiable Data Breaches Report: [Notifiable data breaches publications including January – December 2022](#)

Power to the people: taking back control

Well, maybe not a firm ‘no’, but heightened awareness of privacy risks has shifted how people feel, they’re now more cautious than ever about sharing personal information and more anxious about the type of information organisations are requesting.

56% of our respondents say they’ve been required to provide more personal information than necessary in the past year. They’re particularly concerned about identity documents, with 74% expressing strong preference against organisations collecting or retaining this type of personal information. Put best by a member of our focus group, “Companies make it too complex to control our own data.”

As a result, consumers are increasingly restricting the personal information they share. 52% of consumers have chosen not to complete non-mandatory form fields and 35% have chosen not to buy a product or service when an organisation asked to collect personal information they weren’t comfortable sharing.

Our Deloitte research found the education and employment sector (84%) and the travel and transport sector (83%) consistently collected more personal information than required. The retail sector was considered least likely to collect more personal information than necessary (60%).

Generational differences

Our research found that older generations (50-and-over) traditionally look to organisations and the government to initiate change and safeguard consumer privacy. This is reflected in how the generations respond to a data breach. For our older generations who had experienced a breach, anger towards the organisation (32%) was twice that of under-35s (15%).

Overall, 40% of respondents said the organisation’s response made them feel neither better nor worse. However, there were significant differences among the generations.

36% of under-35s said the organisation’s response made them feel better, while 28% said that it made them feel worse. In contrast, only 16% of consumers aged 50-and-over said the organisation’s response made them feel better, while 47% said it made them feel worse.

Older consumers were also less accepting of organisations experiencing a second data breach, with just 5% saying it’s unfortunate but understandable, compared to 21% of those under-35.

But it would be a mistake for organisations to think the younger generations are laissez-faire about privacy. Under-35s may be more forgiving of organisations around data breaches, but they’re also more likely to take the initiative to address issues themselves rather than wait for others to solve them.

For those who have experienced a data breach, 45% of under-35s have proactively left a provider, compared to 26% of those aged 50-and-over. They’re also taking matters into their own hands by actively engaging in privacy-conscious behaviour, such as using encrypted communication apps, employing ad-blockers and managing privacy settings on social media platforms.

This generational shift shows that organisations need to go beyond the basics of meeting regulatory mandates and give people greater control over their personal information. By embracing cutting-edge tools and methodologies that safeguard sensitive data, organisations can meet younger generations’ higher standards and build a culture of trust, transparency and responsible data stewardship.

Benefits of this approach will reach far beyond organisations’ own walls and help strengthen the wider privacy landscape.



refused to buy a product/service when asked for personal information they weren’t comfortable sharing.

Top 3 consumer privacy protection steps

In the last six months the top steps our survey respondents took to protect their privacy were:



Changing or updating passwords for online accounts and services (67%), with 14% planning to do so in the next six months.



Refusing to share personal information over the phone with an organisation (56%), with 14% planning to do so in the next six months.



Limiting the personal information, they share with brands (56%), with 17% planning to do so in the next six months.

Chapter 2 | The privacy pursuit: What the public wants

We know how people are feeling about privacy, breaches and the actions they're taking to get control of their data, but where else do they want change and action?

- i
- ii
- iii
- iv
- v
- 1
- 2
- 3

It will come as no surprise that most of our respondents (90%) agree that more should be done to protect data, but what exactly do people want done and by whom?

“What do we want?”
“Rules, reforms and responsibility!”
“When do we want it?”
“Now!”

It’s not the most electrifying battle cry, but when it comes to their privacy almost all people expect significant action from governments and organisations.

Interestingly, when analysing the age demographics, the stats show that **82%** of young people agree more should be done to protect data, slightly lower than the overall agreement rate of **90%**. Conversely, the agreement rate rises to **96%** among older people, reflecting their heightened concerns regarding data security and privacy.



What consumers want from the government

Australia’s privacy reform review is ongoing and it’s not yet clear what specific changes will be made to the country’s privacy laws. However, our survey results suggest there’s significant public support for stronger privacy protections. 86% of our respondents believe new rules and regulations around data storage and processing are needed and 63% believe it’s the government’s responsibility to maintain standards and regulate data storage and possession.

Specifically, our survey participants and focus groups want the Federal Government to:

- Create a regulatory body to verify organisations are ethical data companies with a public-facing label to certify this.
- Mandate organisations are transparent and proactive in communicating about their data-handling practices and where data is stored, plus simplify privacy policies and use easy-to-understand language.
- Set time limits on the amount of time organisations can hold consumer data.
- Make businesses accountable when data breaches occur.

What consumers want from organisations

Overall, consumers want organisations to be held accountable for data breaches. 80% of consumers agree if their data is exposed by a breach the organisation should compensate victims individually for the potential harm and inconvenience. They also want organisations to be more transparent about how they handle their data. Our participants believe it’s important organisations explain:

- **Why (91%)** they require their personal information
- **How (92%)** they will use their personal information
- **Who (94%)** they will share their personal information with.

The Office of the Australian Information Commissioner (OAIC) is the country’s federal privacy regulator.

There are also a number of state and territory-based and industry regulators in Australia that oversee privacy and data protection.

What people want from organisations versus what they're getting

	What they want	What they're getting
 Data collection	The right to object 93% of consumers say it's important to have the right to object to an organisation collecting and using their personal information.	According to our research, only 11% of organisations mention the ability to object in their privacy policy.
 Data usage	Data respect! 95% say it's important their information isn't sold to third parties.	Our organisation analysis found that 79% of organisations make no mention in their privacy policy whether personal information is sold or not.
 Data storage	Transparency 90% of our survey participants say the main driver to trust an organisation with their personal information is for organisations to explain clearly and transparently how they will store information and maintain consumers' privacy.	Only 8% of organisations provide accessible privacy policy engagement options beyond plain text format (such as video, audio or infographics). 27% are written in legal jargon without explaining what these privacy concepts mean in the context of their organisation's use of data. Only 6% provide additional content to help people understand what they're signing up for.
 Data deletion	Easy deletion 93% say it's important to be able to request organisations delete their data.	Our analysis indicated only 17% of organisations mention giving people the option to erase their data.



Data deletion (cont.)

Of the 17% of organisations that mention the option to delete their personal information:

- 2% said they would delete a consumer’s account and personal information after a period of inactivity.
- 7% said they would deactivate the account but retain the personal information.
- 41% said they would only delete the account at the consumer’s request.
- 50% provided no option or reminder to delete the account after a period of inactivity.

We also discovered that consumers are confused about how data retention works. Focus group participants said they, **“Had no idea what the process/policy is around data retention.”** This confusion could be contributing to their perception that organisations are, **“Intentionally making data deletion inaccessible and a complicated process”**.

Our organisational analysis shows there’s a disparate approach to managing consumer accounts and personal information – ranging from minimal proactive measures to the absence of deletion options. With the ‘right to erasure’ currently being debated as one of the Privacy Act 1998 (Cth) amendments, this disparate approach highlights how ill-prepared organisations are for upcoming privacy regulatory change.

Urgent actions for organisations

To address these gaps organisations must take urgent action to implement consistent and robust data protection practices that emphasise data minimisation, proactive deletion strategies and a consumer-centric approach.

By aligning policies and practices with evolving privacy regulations, organisations can ensure compliance and foster greater consumer trust and uphold the principles of data privacy in an increasingly interconnected digital landscape.

“I had no idea what the process/policy is around data retention.”

“Organisations make data deletion inaccessible and a complicated process”

- Focus group participants

Chapter 3 | What now for organisations?

We've taken the nation's pulse, we know what people want and from whom, but what does it mean for Australian organisations?

In this chapter, we use our survey and focus group insights and add our specialists' research and analysis to look at how organisations can meet and exceed consumer expectations.

i

ii

iii

iv

v

1

2

3

The people’s message is loud and clear: organisations must do more to protect personal information.

Organisations have everything to gain by listening to consumers concerns – by understanding how people are feeling, looking at key stats and putting strategies in place to minimise data breaches, they can build trust and loyalty.

The flip side of this, is loss of trust, reputational damage, potential legal repercussions and financial consequences.

So where to from here?

Prioritise privacy protection

The first thing for organisations is to prioritise privacy and data security so they can quickly adapt to meet consumer demands. As we know, data and privacy breaches are on the rise, so regardless of size or industry, prioritising the protection of personal information is crucial.

But organisations must aim much higher than just implementing and maintaining strong security measures. The goal is to mitigate the risks of personal information being compromised, so strict strategically-applied safeguards are needed to achieve this, including:



A steadfast commitment to bolstering defences against potential threats.



Reducing risks and areas of vulnerability through data minimisation.



A detailed plan of action – tailored to the specific needs and risks of the organisation – in the event of a breach.

All safeguards and plans should be reviewed and updated regularly to address emerging threats, changes in technology and regulatory updates.

i

ii

iii

iv

v

1

2

3

Data-breach action plan

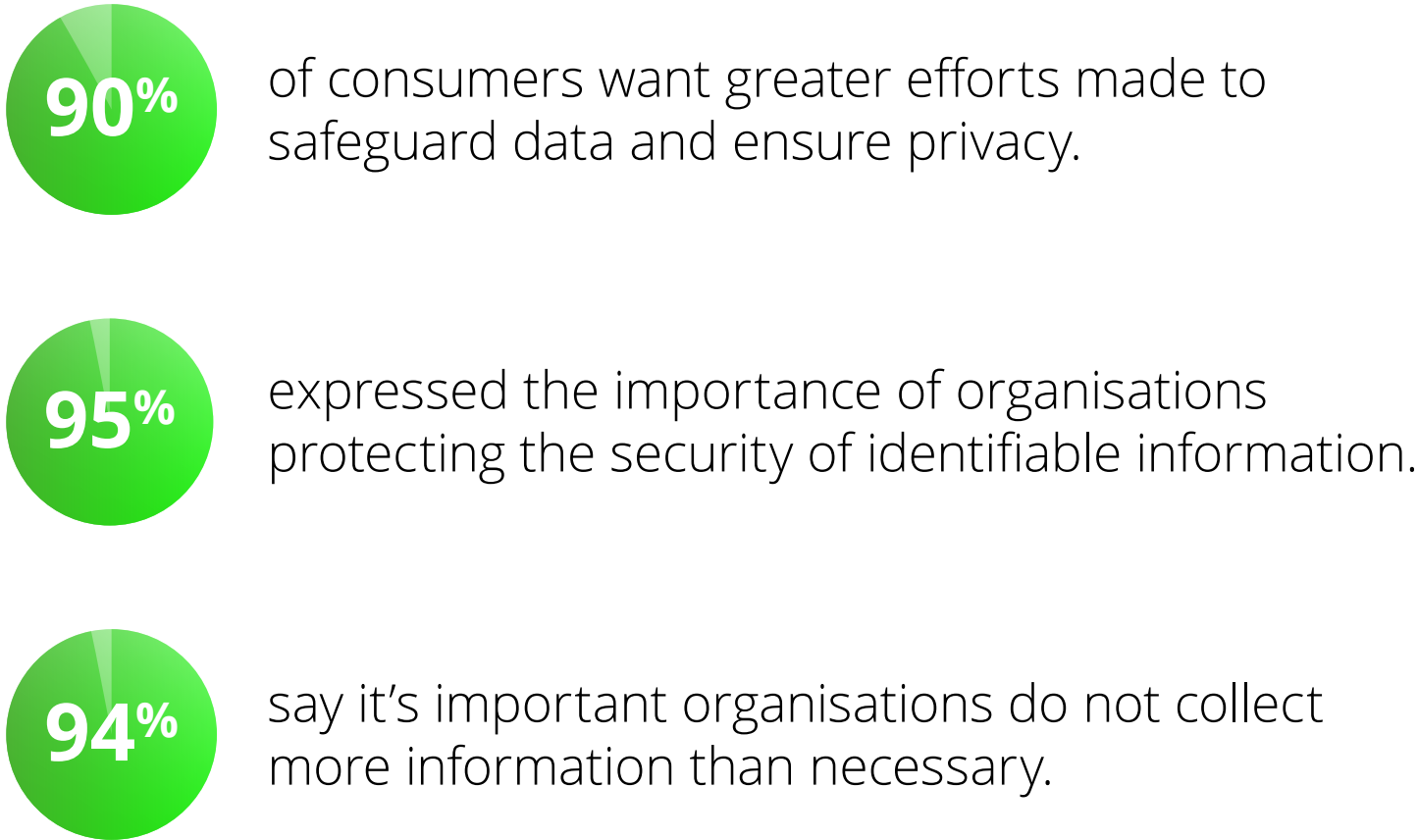
A carefully crafted and comprehensive action plan will guide an organisation’s response in the event of a data breach. The plan should be tailored to the specific needs and risks of individual organisations and include steps for immediate containment, investigation, communication and regulatory compliance.

Privacy protection essentials

Robust protection measures: such as encryption, access controls and regular security audits are essential in reducing breaches occurring. By incorporating privacy-by-design principles, organisations can demonstrate commitment to safeguarding customer information and preventing unauthorised access, use, modification and disclosure.

Risk minimisation strategies: play a pivotal role and rather than just relying on prevention and detection, comprehensive risk minimisation strategies to respond to a breach must also be a key focus. This includes developing incident response plans, conducting thorough breach simulations and fostering a culture of resilience within the organisation. By accepting that breaches are an unfortunate reality, organisations can better allocate resources towards rapid detection, containment and swift response to limit the potential damage.

Data minimisation: is a fundamental privacy principle and practice requiring organisations to only collect and retain the minimum amount of personal information necessary for a specific purpose.³ With 56% of our survey respondents saying they’ve been required to provide more personal information than necessary in the past year and 62.8% saying it’s ‘very important’ brands don’t collect more information than necessary to provide good service, data minimisation has emerged as a key strategy for rebuilding consumer trust, as it reduces risks associated with data breaches.



Privacy-by-design principles
Ensuring privacy and data protection are factored into design and development of systems, products and services from the start.

³ <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>

Put people first: a consumer-centric approach

When reviewing current practices and planning privacy-improvement strategies, organisations should view each step through consumer eyes.

If you were a consumer, would you find your organisation’s practices helpful or frustrating?

Would an average consumer understand or want to read 20 pages of policy?

Would you be happy handing over the data you’re requesting from others?

Regulations will continue to evolve and become more stringent, but a consumer-centric approach that embraces privacy-by-design principles can help future-proof organisations from regulatory reforms and enhance customer relationships.

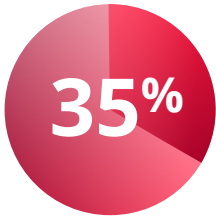
At the opposite end of the spectrum, organisations that fail to meet current consumer expectations risk losing consumer trust and falling further behind when reforms are implemented. To avoid being caught off guard, organisations should proactively assess and address the gaps between existing practices and consumer expectations.

Give people agency

Going forward, providing consumers with a sense of data autonomy by giving them choices on how their data is handled is essential for building trust, transparency and engagement and helping mitigate risk.

However, our organisation analysis shows that currently 35% of organisations do not obtain consent for collection and handling of personal information and 70 organisations don’t let consumers review consent given or withdraw their consent, including where it is likely to be required by law.

Savvy organisations will empower customers to make their own choices around privacy and personal information and even involve customers in the development of privacy policies.



of organisations don’t obtain consent for collection and handling of personal information.



Some ways organisations can *empower* consumers



Consent

- Make it easy for customers to find and understand their privacy practices. Privacy policies or privacy-related content should be prominently displayed on websites and apps.
- Provide clear, transparent privacy policies/ content: use simple, easy-to-understand language. Customers should be able to understand their privacy rights without consulting a lawyer.
- Make it easy for customers to access and control their personal data – they should be able to opt-out in just a few clicks.



Usage

- Be transparent around data usage. Customers should know how their data is being used and for what purpose and whether data will be shared with or sold to a third party.



Deletion

- Make it easy for consumers to request their data be deleted.
- Be proactive about deleting data after a period of inactivity.
- Be clear about data retention policies, so consumers know how long personal information will be kept and why.

i

ii

iii

iv

v

1

2

3

Say it how it is: communication is key

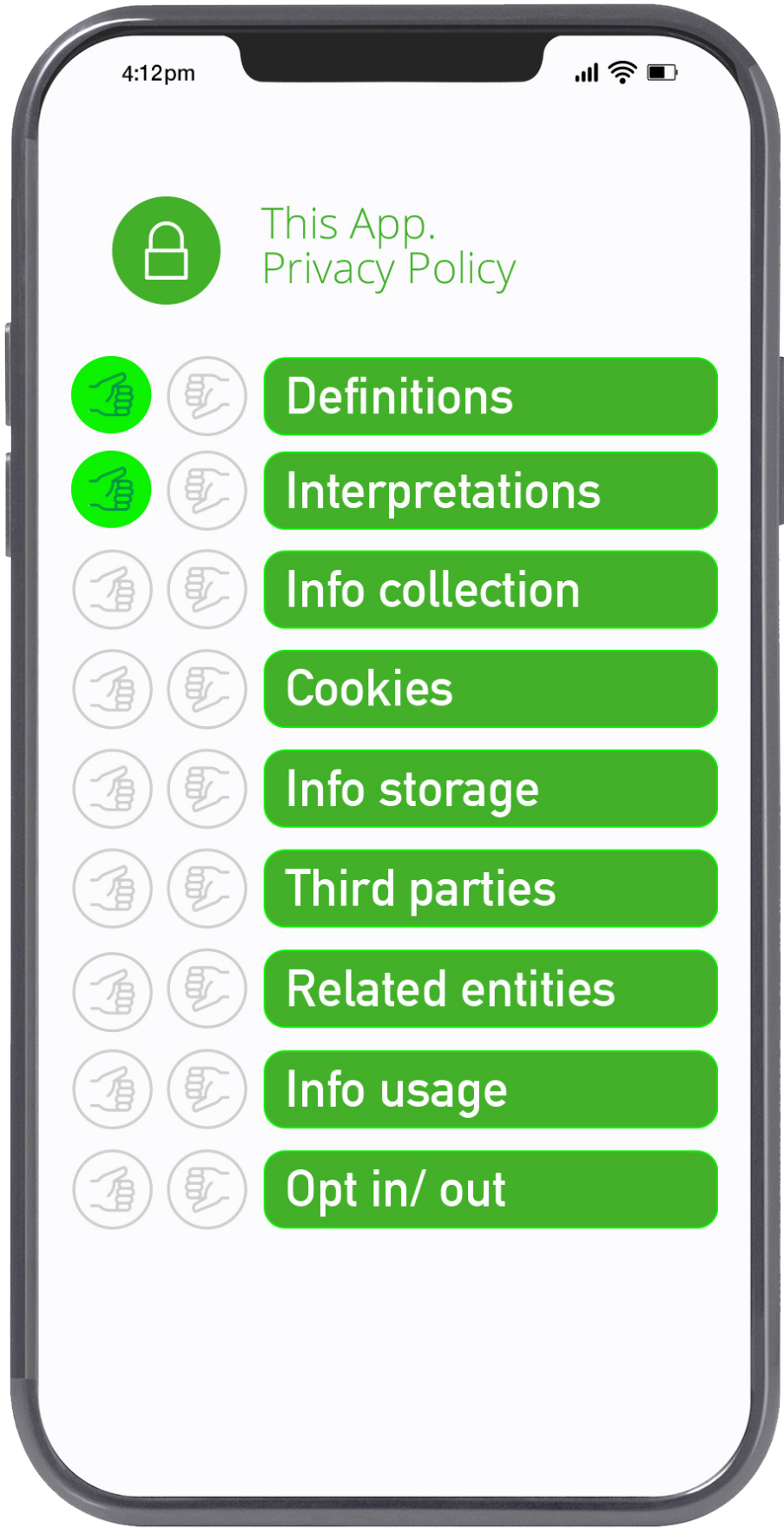
In a world where consumers wade through complex, tedious privacy policies for key information, organisations have an opportunity to foster trust, enhance transparency and differentiate themselves by creating compelling privacy content that empowers and reassures customers.

Firstly, it’s time to ditch long, legal privacy policies and adopt easy-to-understand, easy-to-access communication that clearly explains privacy practices. This should include information on data collection, use, retention and deletion, specifying data types, purpose, duration and addressing data sharing or selling, as well as how stored data will be protected. We made similar observations in previous Privacy Index reports, highlighting the need for organisations to start acting and step up.

By delivering interesting, engaging content through diverse mediums like video and audio across different platforms, organisations can connect with customers, irrespective of age, digital proficiency or abilities.

Content can be created for different audiences or address particular concerns, giving consumers a clear understanding of data practices, informed consent, greater control, reduced anxiety and an improved user experience. Creating trust in organisations and confidence for their customers.

By raising the bar through compelling content, organisations can enhance transparency, compliance and brand perception, leading to stronger relationships with customers and a competitive edge.



Invest in technology

As data breaches increase in frequency and sophistication, conventional methods are no longer enough and new innovations and technology must be explored.

Australia is lagging behind other countries in awareness, support and uptake of **privacy-enhancing technologies (PETs)**, which can anonymise and encrypt data and prevent data-sharing without user consent. Over the past 12 months, the Singaporean government has adopted PET Sandbox which lets businesses securely test PET projects, the US and UK governments ran a joint PET challenge initiative where innovators competed for cash prizes by developing PET solutions. Also in the US, there was overwhelming bipartisan support for a Bill to support research on PETs and promote responsible data use.

Organisations that share large volumes of data – particularly special category data – should start the discussion about adopting privacy-enhancing technologies (PETs).

Regulators around the world are also starting to embrace innovative PETs. **Homomorphic encryption** and **secure multiparty computation (MPC)** are two proven PET solutions.

Homomorphic encryption lets people work on encrypted data without it having to be decrypted. It enables secure data analysis and processing while maintaining the confidentiality of sensitive information. This technology is revolutionising the way businesses handle customer data, ensuring that even in the event of a breach the data remains protected.

MPC lets multiple parties collaborate and compute results on their combined datasets without disclosing individual data. By securely conducting computations across multiple entities, MPC ensures privacy while deriving valuable insights from collective data. This approach significantly minimises the risk associated with sharing sensitive information and fosters a collaborative environment without sacrificing individual privacy.

Consent management platforms (CMPs) are another tech solution helping companies collect and manage user consent for data collection and processing. There are now a range of ready-to-go CMP and PET solutions that organisations can easily implement to help protect their users' privacy.

Going forward, government, business and organisations will have to work together to advance Australia in this space. By fostering a collective culture of innovation, the country can keep pace with the latest technology and create a dynamic environment, encouraging creative local solutions for global challenges.



i

ii

iii

iv

v

1

2

3

It takes a village:
a collaborative approach to privacy

Privacy affects all of us and to move into a new, improved era of privacy and data protection, we must all play a part. Effective change will need active engagement from organisations, government and individuals.

Australians can play their part by being proactive with privacy and their personal information, this could be staying informed about data privacy, using strong passwords, regularly reviewing and adjusting app permissions, limiting data sharing, reporting suspected breaches to relevant authorities or platforms and supporting privacy-conscious companies.

Government must continue playing an active role – to create and enforce policies that foster a secure digital environment, to align with consumer expectations and work with organisations to achieve rigorous standards and promote transparency in data-handling practices.

For **organisations**, merely meeting regulatory requirements isn't sufficient. A proactive approach must be adopted, one that goes beyond compliance to embrace a culture of privacy and security. Privacy shouldn't be seen as legal obligations, but essential components of building trust and maintaining customer loyalty. By prioritising consumer expectations and proactively working to protect consumer privacy, organisations can navigate the evolving privacy landscape while fostering a culture of data protection and trust and also gaining or maintaining a competitive edge.

For many organisations, privacy seems to fall between the gaps of the customer teams (digital and marketing), risk teams (legal and compliance), cyber security and technology teams (data and technology).

All have a different view on the severity of the situation and how best to respond. True change and leadership for organisations will only occur with these functions acting in unison and prioritising the needs and wants of their customers.

Privacy risks – including identifying risks, implementing controls and ongoing monitoring - should be assessed and managed by a cross-functional team, with members from legal, marketing, IT and customer service. They should provide regular updates to senior management.

Top-tier accountability is also crucial. A Chief Privacy Officer (CPO) should oversee compliance with data privacy laws, develop the privacy program and ensure adherence. This commitment builds trust, prevents breaches and minimises fines, benefiting customers, employees and stakeholders.

The final word will go to consumers.
What will it be for your organisation:
'opt-in' or 'opt-out'?

i

ii

iii

iv

v

1

2

3

Contacts

Partners



Kate Monckton

Partner | Risk Advisory | Sydney
kmonckton@deloitte.com.au



Daniella Kafouris

Partner | Risk Advisory | Melbourne
dakafouris@deloitte.com.au



Lucy Mannering

Partner | Risk Advisory | Sydney
lmannering@deloitte.com.au



Mat Norton

Partner | Deloitte Digital | Melbourne
matnorton@deloitte.com.au



David Phillips

Partner | Deloitte Digital | Melbourne
davphillips@deloitte.com.au

About the team

The Privacy specialists in our Cyber Risk Practice who developed the Deloitte Australian Privacy Index 2023 included:

Lead Partner

Kate Monckton

Lead Director

Tim Scott

Project Manager

Teagan McKenna

Project Co-ordinators

Samantha Barr, Divya Kanagasabapathy, Dina Gouda

Project Writers

Kate O’Brien, Sonia Widjaja, Alcina Giang, Galen Ou and Catherine Guo

Research

Tahlia Pelaccia, Anushiya Achudhan, Joshua Cutrone, Lucy Goodin, Liam Price, Thenuga Rajeswaran, Yassie Malekloo and Georgia Ryan

With thanks to Deloitte Digital for their contribution to our research and report

Anna Fox, Kristen Vhranas, Lucy Baker, Thomas Odgers, Peta Abelardo, Frances Curtis and Taylor Brodie.

i

ii

iii

iv

v

1

2

3

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organisation”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organisation”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organisation”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 415,000 people make an impact that matters at www.deloitte.com.

About Deloitte Asia Pacific

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

About Deloitte Australia

The Australian partnership of Deloitte Touche Tohmatsu is a member of Deloitte Asia Pacific Limited and the Deloitte organisation. As one of Australia’s leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, risk advisory, and financial advisory services through approximately 14,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at <https://www2.deloitte.com/au/en.html>.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

© 2023 Deloitte Touche Tohmatsu

1075604865_Designed and produced by The Agency | Deloitte Australia_08/23