Deloitte.

Australian Retail Association: Privacy & Consent

November 2023

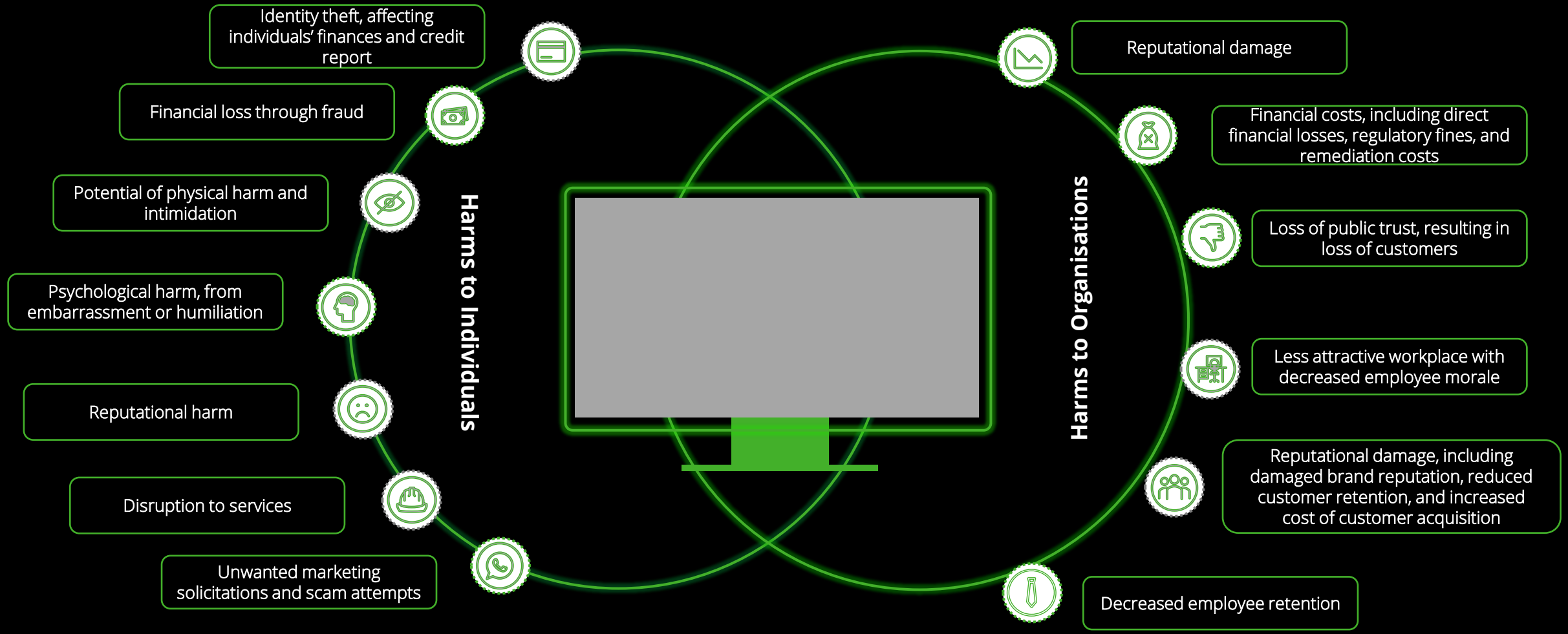
Contents

Cyber lessons learnt?

What we can share about recent breaches and how to best respond

Aftermath of a Data Breach

Impacts to the *organisation and individuals…*



The Changing Privacy & Consent Landscape

How is the landscape evolving?

Drivers for change

Ready or not, the landscape is evolving. It is imperative Marketers, agencies, publishers and platforms make structural changes to prepare for data driven marketing in 2023 and beyond. These changes will involve risks, but failing, or choosing not to act, is just as (if not more) risky.

Changing Consumer Expectations

- Consumers are **becoming more aware** of how companies are using their data and expect **greater transparency**
- Consumers have **a lack of trust** due to public data breaches
- Consumers **expect more value in exchange** for their data

Impact to customer experience and brand trust

Regulatory Reforms

- Reforms across Asia-Pacific and Australia, will bring an increase in customer autonomy, tighter controls around personal information collection and destruction. Greater focus on keeping consent current and specific.
- These reforms reflect thematic shifts in privacy regulation and are expected to influence state-based regulation in the near future.

Impact to privacy and consent practices

Changes to Tech & Data Landscape

- Apple eliminated 3rd party cookies, Apple IDFA, and IOS restrictions.
- Google Chrome is set to remove 3rd party cookies.
- Upwards of **70% depletion of 3rd party cookie data** used for targeting
- Cyber criminals are becoming more sophisticated

Impact to acquisition marketing and measurement

Deloitte Australia Privacy Index 2023

About the *report…*

Index Methodology

- **7th** year in a row
- **100** leading Consumer Brands were assessed
- We surveyed **1000** people across Australia
- Qualitative Research with consumer focus groups to understand consumer sentiment
- Theme this year…..

Responsible data handling

Why is this year's index more important than ever…

Cyber Breaches have impacted many consumers and their trust in organisations.

Increased consumer awareness and expectations of management of their data.

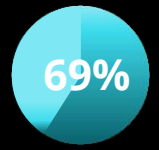
Impending Privacy Reform items to strengthen the Privacy Act require immediate action.

2023 Deloitte Australia Privacy Index – Insight Snapshots

The 2023 *Deloitte Australia Privacy Index* focused on **Responsible Data Handling**, intending to provide a deeper understanding behind consumer sentiment surrounding privacy in the current environment.

INTO THE BREACH

1/3 of consumers have **been affected by a data breach** in the last 12 months



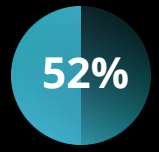
69% of those **felt vulnerable** or **angry** as a result of the data breach

Twice as many consumers were **angry with the organisation (24%) than the cyber criminals behind it (12%)**

80% believe organisations should be **held liable for compensating** data breach victims for potential harm and inconvenience

TAKING BACK CONTROL

56% say they've been required to provide **more personal information than necessary** in the past year



52% have **chosen not to complete non-mandatory** data form fields

35% have **chosen not to buy a product or service** because an organisation asked to collect personal information they weren't comfortable sharing

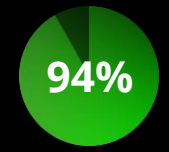
63% of consumers **believe governments should be responsible** for maintaining standards and regulating data storage and possession

WHAT CONSUMERS WANT

90% of consumers **want more done to protect their data**

86% of respondents **want new rules and regulations** around data storage and processing

91% of consumers **want to know why organisations want their personal information**



94% of consumers **want to know who their personal information will be shared with**

2023 Deloitte Australia Privacy Index – Insight Snapshots

What consumers want from *organisations…*

What do consumers want from organisations?

Transparency

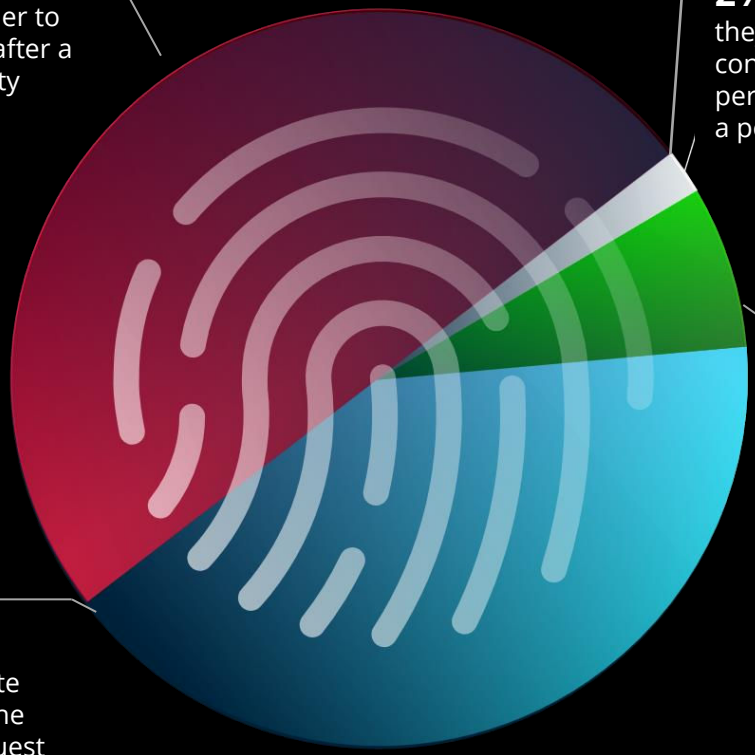
Consumers want organisations to be more transparent about data handling.

Data deletion

Easy deletion – 93% of consumers said it's important to be able to request the deletion of their data.

What they're getting:

Our organisational analysis indicates only **17%** of organisations mention giving people the option to erase their data

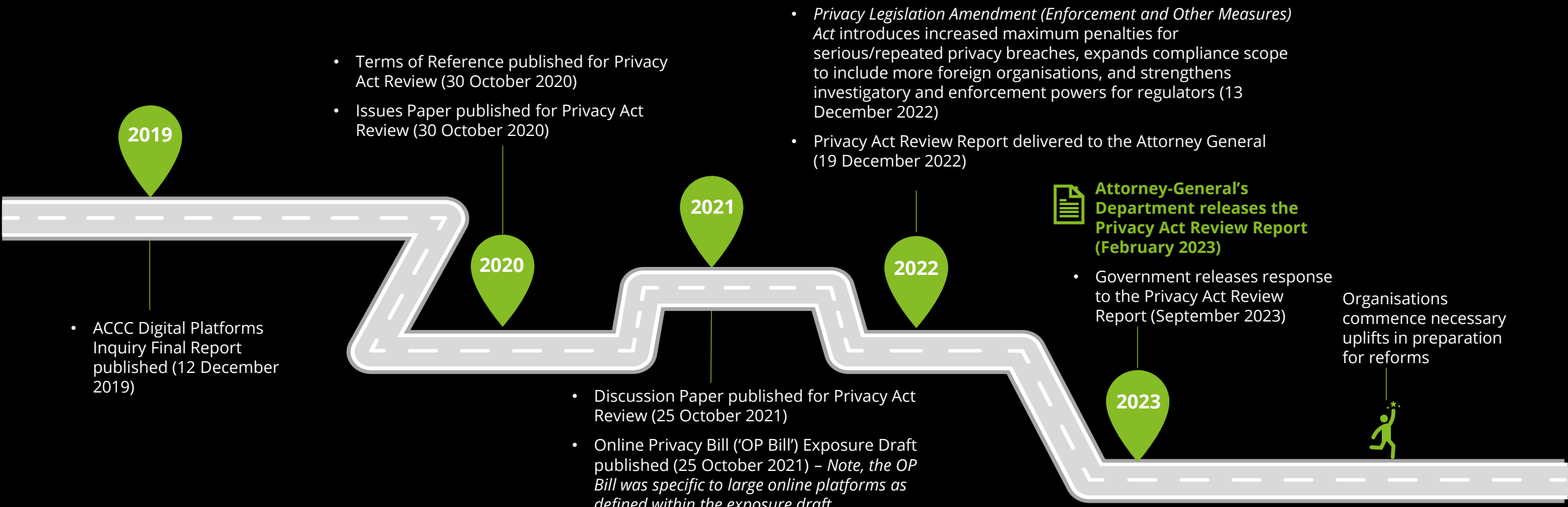


The changes in regulatory reforms

How is the government responding?

The *Privacy Act* review timeline

In 2019, the Commonwealth Government committed to reviewing the *Privacy Act 1988* (Cth) ('Privacy Act'). Outlined below is a timeline of the key milestones from the review.



Contextualising Privacy Act Reforms

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte highlights a snapshot of 10 key proposed changes which are likely to have significant impact on business operations.

1. Expanded definition of personal information (PI)

2. Strengthened consent requirements

3. Enhanced protections for employee personal information

4. Introduction of new individual rights (e.g. right to be forgotten / erasure)

5. Strengthened controls for data sharing and overseas data flows

6. Shorter timeframes for data breach notification

7. Enhanced security protections for personal information

8. Additional rights and protections for targeted marketing

9. Introduction of a 'fair and reasonable' test for privacy and consent policies

10. Transparency and review of retention periods

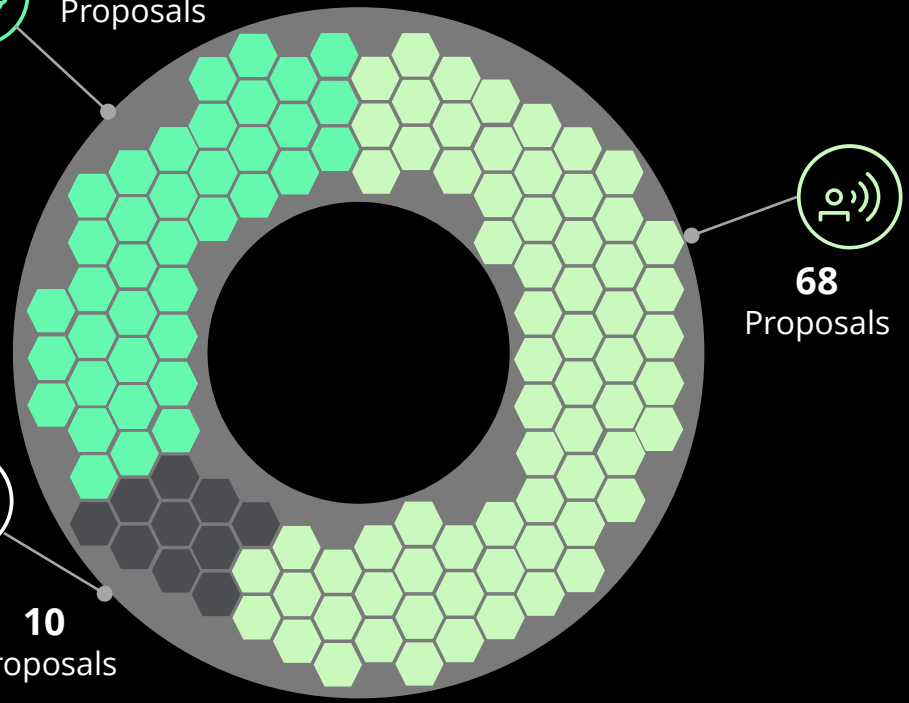
Summary of the Government Response to the *Privacy Act* Review

The Australian Government provided a response in September 2023 which categorises each proposal, but more critically provides an insight into the Government's rationale behind the categorisation provided, enabling organisations to progress preparation activities with further certainty around the potential impact of the proposed reforms.

Agreed

Proposals denoted as agreed by the Government will be progressed to the development of legislative provisions, and **organisations can begin to prepare for these to be introduced.**

38
Proposals



68
Proposals

Agreed-in-Principle

Proposals denoted as agreed-in-principle by the Government are to be subject to further refinement. **Organisations should begin to consider the impact of these being introduced,** utilising the themes of the proposals and associated commentary assist in understanding what may be done.

Noted

Proposals denoted as noted by the Government are unlikely to be progressed further

10
Proposals

The Impact of getting Privacy *'Wrong'*

What is the significance of the privacy landscape changes to each persona within your business?

Financial Risks

$4.1 Million — The average cost of a data breach for Australian organisations in 2023 [1]

$60 Million — ACCC penalty to Google under Consumer Law for misleading and deceptive conduct, relating to personal information collection [6]

5% — Average stock price underperformance for organisations who suffered a data breach, up to six-months after a breach [3]

1,700 — Number of enforcement actions issued across Europe in the five-years since introducing the GDPR [9]

Reputational Risks

25% — Proportion of cost impacts relating to *lost value of customer and member relationships* felt by an organisation who suffered a breach of personal and sensitive information [3]

Customer Risks

49% — Proportion of customers who indicated their desire to remain a customer was dependent on the assurances a brand can provide following a breach [4]

86% — Proportion of customers who indicated timely notification of a breach would impact their trust with the brand [4]

10% — Increase in complaints received by the industry regulator, the TIO, following the Optus breach – all of which require engagement and review by the provider [5]

Operational Risks

277 Days — The average global response time for a breach - 207 days to identify the breach, and 70 days to contain it[2]

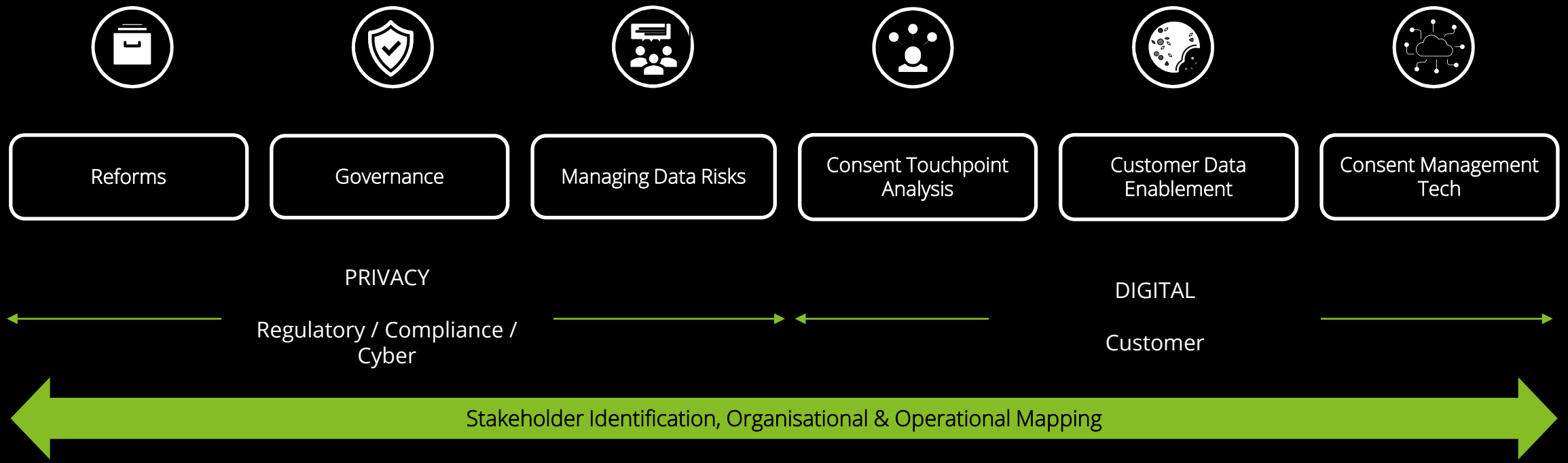
25% — Proportion of cybersecurity leaders who will pursue different roles entirely as a result of workplace related stressors [8]

50 — Organisations who have had *negative credit rating actions* (a downgrade in rating, or negative revision in outlooks), with attribution to cyber attacks. [7]

Where to start?

Where to start - Key areas of Privacy and Consent

We understand the privacy & consent topic is complex. We leverage a “whole of organisation” approach by ensuring all six streams are considered, we need to run a diagnostic assessment to develop a roadmap and prioritise



What does best in class look like?

There are common features of a best-in-class program that functions to support organisation-wide commercial objectives and also aligns to privacy obligations, taking into account risk appetite.

Organisations that do this best feature the following…

Establish a clear strategic balance of commercial objectives with compliance and risk.

Create a strategic imperative at the Executive level.

Integration and collaboration of internal functions with shared ambitions.

Establish metrics and reporting on consent rates and unsubscribes shared across the business.

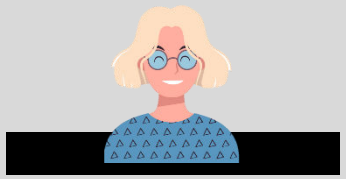
Clear accountabilities and responsibilities around PI capture, usage and deletion.

Optimise technology capabilities and enablers to allow for agile operations.

Clear focus on customer experience and brand drivers

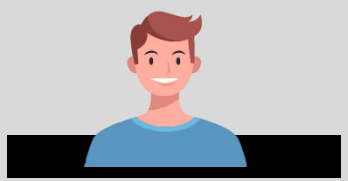
Solving Privacy and Consent Management across the Enterprise

What is the significance of the privacy landscape changes to each persona within your business?



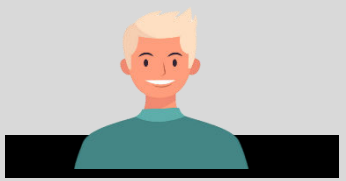
Chief Privacy Officer

- How is my organisation preparing for the changes?
- Who do I need to influence to get the appropriate budget allocations?



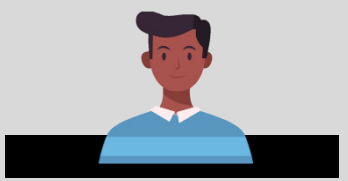
Chief Marketing/Digital Officer

- How will I have to change my marketing , advertising and consent practices, technology and processes?



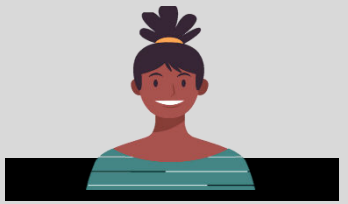
Chief Technology Officer

- How will our technology solutions be impacted?
- What can I do now to future proof?
- How will this impact my transformation programs?



Chief Information Security Officer

- How will I need to protect personal information differently?
- Are we ready for a 72-hour breach notification requirement?



Chief Data Officer

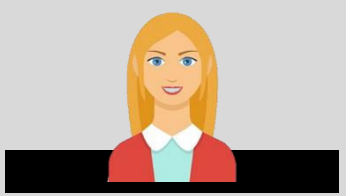
- Do I know where our PI is and how long we should be retaining it for?
- What data will be considered PI that currently isn't?

Board Director

- Do we have the right skill set on, or advising, the Board to understand and meet our director duties?

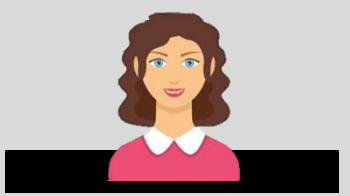
Chief Financial Officer

- What are the costs of compliance uplift?
- What are the recovery costs if we have a breach – operational, fines, compensation?



Chief Risk Officer

- Do we understand our privacy risks across the organisation and how these may change?
- Do we have an agreed privacy risk appetite?



Chief Executive Officer

- How do I know we are meeting our customer, Board, employee and regulator expectations?
- Do I feel confident in our breach response plans and communications?

Chief Customer Officer

- How are we communicating our privacy practices to our customers in the most effective ways?
- How will we prepare for increased customer requests?

Thank you

To learn more about what we discussed today

Daniella Kafouris
Partner
E: dakafouris@deloitte.com.au

David Phillips
Partner
E: davphillips@deloitte.com.au

Download the full *Privacy Index Report*

Scan to download the report

Appendix 1 : Privacy Index Report

Deloitte Australia Privacy Index 2023

How consumers are *feeling...*

Into the breach

1/3 of consumers have been directly affected by a **data breach** in the **past 12 months**.

69% of those impacted felt **vulnerable** or **angry**.

80% of people believe organisations should be **held liable for compensating** data breach victims individually for the potential harm and inconvenience.

47% of people **aged 50+** said organisations' **response** made them **feel worse**.

36% of people **under 35** said the organisations' **response** made them **feel better.**

2x

as many people were **angry** with the **organisation** (24%), rather than the **cyber criminals** behind it (12%).

Deloitte Australia Privacy Index 2023

What are consumers *doing...*

The privacy pushback: taking back control

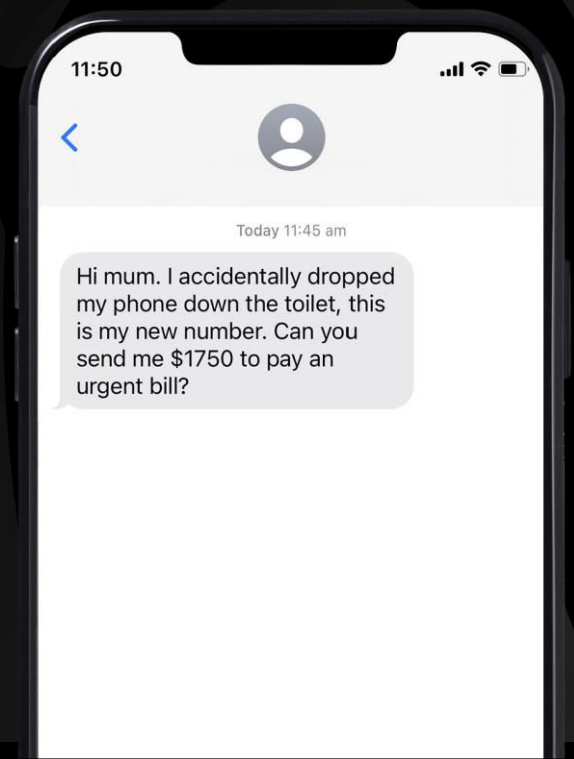
56% say they've been required to provide **more personal information than necessary** in the past year.

52% of consumers have chosen **not to complete** non-mandatory form fields.

35% have **chosen not to buy a product or service** because an organisation asked to collect personal information they weren't comfortable sharing.

45% of under 35s have **chosen to leave a provider after** experiencing a **data breach.**

Younger generations are taking matters into their own hands by actively engaging in privacy-conscious behaviours.



Deloitte Australia Privacy Index 2023

What consumers are *wanting...*

Action stations: what people want

of people want **more done** to protect their data.

of respondents want **new rules and regulations** around data storage and processing.

believe it should be the **government's responsibility** to maintain standards and regulate data storage and possession.

Transparency: people want to know **why (91%) organisations** want their personal information, **(92%) how it will be used** and **who (94%)** it will be **shared** it with.

Appendix 2 : Privacy Reforms - What can we begin to prepare for?

What can we begin to prepare for?

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte has compiled a view of what organisations can begin to do in order to reduce the operational burden imposed by the reforms, while remaining cognisant of the ongoing changes that may occur.

What is changing?

APP Codes - Proposals 5.1 & 5.2 – The Government agrees that the ability for the Information Commissioner to make an APP code on the direction or approval of the Attorney-General should be enhanced. This will enable the Information Commissioner to respond in circumstances where it is in the public interest for a code to be developed and there is unlikely to be an appropriate industry representative to develop the code or it is urgently required.

- There will be limited immediate impact of the proposed enhancements to the Information Commissioner's ability to make a Code under the APP, however, organisations operating in specific industries should have sufficient flexibility and maturity in their privacy programs to ensure the ability to adhere to additional requirements that may be introduced in addition to the APPs.
- There are existing APP Codes in place for Credit Reporting, Market and Social Research, and Government Agencies, with consultation undertaken on proposed codes for Online Platforms.

New Technology - Proposal 13.3 – The Government agrees the OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks.

- Ensure there are strong privacy governance procedures in place to conduct and document Privacy Impact Assessments ('PIAs') and/or risk assess all organisational practices that utilise personal information with new technologies or that may involve emerging privacy risks.
- Undertake, or ensure, privacy and risk assessments have been conducted over all existing organisational practices that involve the use of new technologies or may introduce emerging privacy risks.

Children - Proposal 16.1 – The Government agrees that a child should be defined in the Act as an individual who has not reached 18 years of age.

- Ensure you know where your organisation currently conducts, or you have mechanisms in place to prevent, the collection or handling of personal information from individuals under the Age of 18 and this is tracked.
- Implement or enhance mechanisms to determine whether parental/guardian consent is required and ensure considerations around children are built into the broader organisational privacy program. Undertake, or ensure, privacy and risk assessments have been conducted over all existing organisational practices that involve the use of new technologies or may introduce emerging privacy risks.

What can we begin to prepare for?

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte has compiled a view of what organisations can begin to do in order to reduce the operational burden imposed by the reforms, while remaining cognisant of the ongoing changes that may occur.

What is changing?

Children's Online Privacy Code - Proposal 16.5 – To clarify how the best interests of the child should be upheld in the design of online services and provide further guidance on how entities are expected to meet requirements regarding targeting, direct marketing and trading, the Government agrees a Children's Online Privacy code should be developed (proposal 16.5) as soon as legislated protections for children are enacted to enable the development of such an APP code. The code would apply to online services that are likely to be accessed by children.

- ❑ Ensure there are strong privacy governance procedures in place to conduct and document PIAs and broader consultation on all organisational practices that utilise the personal information of children, including specific consideration of mechanisms that will ensure online services used by children are designed in a manner that are in their best interests.

Vulnerable Individuals - Proposal 17.1 – To provide additional protections for individuals who may be experiencing vulnerability or may be at higher risk, the Government agrees OAIC guidance should include a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

- ❑ Ensure existing privacy governance procedures properly consider the risks associated with collecting or handling the personal information of individual's experience vulnerability, including consideration of who these individuals may be in the context of your organisation. This can be primarily directed through privacy engagement points (e.g., PIAs) but should also be considered throughout all aspects of the privacy program (e.g., consent requirements).

Automated Decisions - Proposals 19.1 & 19.2 – The Government agrees that privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal, or similarly significant effect on an individual's rights and that high-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Privacy Act and supplemented by OAIC guidance.

- ❑ Ensure all existing uses of substantially automated decisions are identified, tracked and fed through existing privacy governance mechanisms and are subject to review and result in any required changes to public-facing materials like privacy policies and collection notices.
- ❑ Enhance or develop internal materials to properly consider the meaning of 'substantially automated decisions' and undertake an uplift of privacy education and awareness to ensure all employees handling personal information are aware of where a 'substantially automated decision' may exist.

What can we begin to prepare for?

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte has compiled a view of what organisations can begin to do in order to reduce the operational burden imposed by the reforms, while remaining cognisant of the ongoing changes that may occur.

What is changing?

Civil Penalty Provision - Proposal 25.1 – The Government agrees a new mid-tier civil penalty provision should be introduced to cover interferences with privacy which do not meet the threshold of being 'serious' and a new low-level civil penalty provision for specific administrative breaches of the Act and APPs should be introduced with attached infringement notice powers for the Information Commissioner with set penalties.

- ❑ Ensure privacy programs are adequately integrated into broader risk management programs to identify and manage privacy-related risks across all components of an organisation.
- ❑ Undertake awareness and education for all employees responsible for privacy or risk management to ensure there is an understanding of the various civil penalties that will exist with respect to privacy compliance, including the associated financial and regulatory impacts.

Increased Enforcement - Proposal 25.2 – the Government agrees section 13G of the Privacy Act which deals with 'serious or repeated' breaches of privacy should be amended to remove the word 'repeated' and clarify that a 'serious' inference can include repeated interferences with privacy.

Proposal 25.5 – The Government agrees entities should be required to identify, mitigate and redress actual or foreseeable loss suffered by an individual.

Proposal 25.10 – To ensure the ongoing effectiveness of the OAIC, the Government agrees the OAIC should conduct a strategic organisational review to ensure the OAIC is structured to have a greater enforcement focus.

- ❑ Update your organisations privacy and risk management programs to ensure there is proper consideration of the increased focus on enforcement by the privacy regulator, increased breadth of what is considered an 'interference with privacy' and the additional obligations proposed for organisations to assist in mitigating and redressing loss suffered by individuals.

Notifiable Data Breach - Proposal 28.1 – To ensure data breaches are reported correctly and that entities with multiple reporting obligations are not unnecessarily burdened, the Government agrees further consideration is necessary to determine how best to streamline multiple reporting obligations.

- ❑ Continue to update and test data breach response plans and processes through simulations and/or table-top exercises to ensure effective and efficient functioning prior to regulatory changes, with an aspirational focus on a 72-hour timeline that is in-line with existing obligations across other regulatory frameworks and international jurisdictions.
- ❑ Enhance training and awareness activities across the organisation with respect to data breach management, and ensure staff are educated on what an eligible data breach is and how to report one.

What can we begin to prepare for?

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte has compiled a view of what organisations can begin to do in order to reduce the operational burden imposed by the reforms, while remaining cognisant of the ongoing changes that may occur.

What is changing?

Understanding Automated Decisions - Proposal 19.3 – The Government also agrees that individuals should have a right to request meaningful information about how automated decisions with legal or similarly significant effect are made.

- ❑ Develop additional requirements within your organisation's privacy governance mechanisms to prepare and disclose comprehensive and 'jargon-free' explanations of how 'substantially automated decisions' are made where they are relied upon by the organisation.

Protecting Information - Proposal 21.1 – The Government agrees the Privacy Act's existing security obligations should be enhanced by specifying that 'reasonable steps' in the context of APP 11 include both technical and organisational measures.

Understanding Security Obligations - Proposal 21.3 – The Government agrees the OAIC should provide additional guidance to entities about what reasonable steps an entity should take to keep personal information secure.

- ❑ Ensure there is proper integration of your organisations privacy program with security program(s) to support the protection of personal information.
- ❑ Enhance existing governance mechanisms and internal guidance related to the protection of personal information to ensure there is a mandate to consider both technical measures (which relate to technological methods for protecting information) and organisational measures (which relate to broader instructions, policies and procedures relating to protecting information).

Overseas Transfer Certifications - Proposal 23.2 – The free flow of information across borders is an increasingly important component of international trade and digital service models. While information data flows are critical to economic growth, concerns about the privacy risks of international data transfers continue to grow. To support the free flow of information with appropriate protections, the Government agrees a mechanism should be introduced to prescribe countries with substantially similar privacy laws.

- ❑ Ensure your organisation is able to identify and document all data flows with third parties and interorganisational data flows outside of Australia, including the specific personal information attributes shared to external jurisdictions.

What should you begin to consider?

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte has compiled a view of what organisations can begin to do in order to reduce the operational burden imposed by the reforms, while remaining cognisant of the ongoing changes that may occur.

What is changing?

Definition of Personal Information - Proposals 4.1 & 4.3 – The Government agrees in-principle that amendments to the Privacy Act are needed to clarify that personal information is an expansive concept that includes technical and inferred information (such as IP addresses and device identifiers) if this information can be used to identify individuals. The Government also agrees in-principle that the definition of 'collection' should be amended to expressly cover information obtained from any source and by any means, including inferred or generated information.

- ❑ Where privacy governance processes interact with the proposed expanded definition of personal information (which includes unique identifiers, technical identifiers, as well as inferred and/or generated information), organisations should begin to ensure the privacy management and data protection controls are applied to their collection, handling and disclosure.

The Government's response to the proposed reform includes further OAIC guidance would be developed to clarify whether personal information reasonably identifies an individual in specific contexts.

Employee Records - Proposal 7.1 – The Government agrees in-principle that further consultation should be undertaken with employer and employee representatives on how enhanced privacy protections for private sector employees may be implemented in legislation.

- ❑ Review the organisation's current approach to employee records/personal information and begin to include it within the scope of your organisation's existing privacy program.

The Government's response indicated it would further consult with employer and employee representatives (particularly small businesses) on how enhanced privacy protections for private sector employees may be implemented in legislation, and how privacy and existing workplace relation laws should interact.

Consent - Proposal 11.1 – To improve the quality of consent provided in these circumstances, the Government agrees in-principle that the Act should clarify that consent should be voluntary, informed, current, specific and unambiguous.

- ❑ For collection or handling of personal information that currently rely upon consent, organisations should review the consent mechanisms to ensure they adhere to the new requirement (i.e., should be voluntary, informed, current, specific and unambiguous), aligning its consent practices to established consent standards (e.g. GDPR, CCPA and LGPD).

The Government's response indicated it will need to further consult to determine the specific circumstances the consent requirements should apply to.

What should you begin to consider?

The Government's Response has provided increased certainty around the potential impact of the individual proposals, and assisted in clarifying the intended objectives of the reforms. Deloitte has compiled a view of what organisations can begin to do in order to reduce the operational burden imposed by the reforms, while remaining cognisant of the ongoing changes that may occur.

What has been considered?

Fair and Reasonable Handling – Proposal 12.1 – The Government agrees in principle that this imbalance be addressed through a new requirement that collections, uses and disclosures of personal information are fair and reasonable in the circumstances.

- ❑ Begin to integrate the fair and reasonable test into existing privacy assessments (e.g. a Privacy Impact Assessment) to ensure the collection and handling of personal information aligns with the expectations of customers and consumers.

The Government's response indicated further considerations into the factors that would attribute to the fair and reasonable test will be refined in further OAIC guidance and enforcement actions.

PIAs for High-Risk Processing - Proposal 13.1 – The Government agrees in-principle that non-government entities should also be required to conduct a PIA for activities with high privacy risks and that OAIC guidance should be developed on factors that may indicate a high privacy risk with examples of activities that will generally require a PIA to be completed.

- ❑ Review or uplift the Privacy Impact Assessments ('PIAs') process top ensure documented assessments are conducted on all high-risk or potentially high-risk personal information processing activities.

The proposed reform aims to mandate risk assessment on high-risk or potentially high-risk initiatives. The Government's response indicated an OAIC guidance will be developed to clarify what activities would be considered 'high risk' for new technologies and emerging privacy risks, as well as any guidance to help organisations determine if an activity has a high privacy risk.

Additional Retention Requirements - Proposals 21.7 & 21.8 – The Government agrees in-principle that entities should be required to establish their own maximum and minimum retention periods for personal information they hold and specify these retention periods in privacy policies.

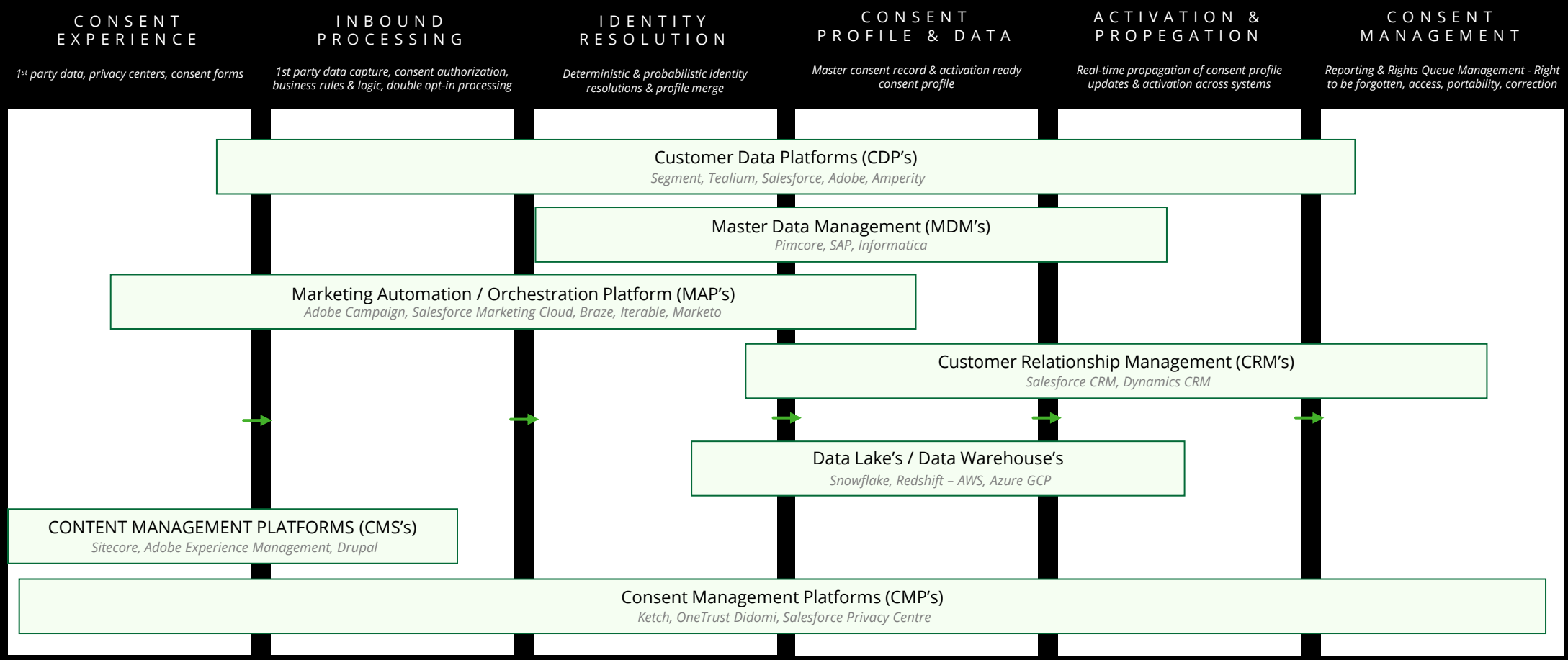
- ❑ Organisations should prioritise addressing any existing backlogs of personal information that may be being held outside of the retention requirements.
- ❑ Reviewing existing retention mechanisms and retention periods to ensure the maximum and minimum retention periods can be identified (i.e., by considering the type, sensitivity and purpose of the information being retained as well as the entity's organisational needs and any obligations they may have under other legal frameworks).

Under existing Australian Privacy Principle 11.2, requirements around retention already exist. However, the proposals around retention will focus on its interaction with other retention requirements and enforcement by the OAIC under its strategic review to have increased enforcement power under proposal 25.10.

Appendix 3 : Consent Management Technology Considerations

Consent requires connected systems

A centralised consent management solution is recommended to ensure consent and preferences are updated **in real-time against a single profile** and activated across relevant digital channels. This solution will provide the **flexibility to continually adapt your consent posture as regulations change.**



Appendix 3 : References

References

Slide: The Impact of getting Privacy *'Wrong'*

Sources:

1. 2022 Cost of a Data Breach Report IBM (Translated to AUD)
    - $1.44 Million USD on Detection/Escalation
    - $1.18 Million USD on Post-breach Response
    - $1.42 Million USD on lost business cost
    - $0.31 Million USD on Notification cost
2. Harvard Business Review
3. 2021 Verizon Data Breach Investigations Report
4. 2018 Privacy Index, Deloitte Australia
5. TIO Quarter Two Complaints Report, 2023
6. ACCC Media Release, Google LLC, 12 August 2022
7. S&P Global, Cyber Trends and Credit Risk, 25 October 2022
8. Gartner 2023, Predicts 2023: Cybersecurity Industry Focuses on the Human Deal
9. IAPP Global Privacy and Data Protection Enforcement Database (ongoing)