Deloitte.

September 2024

Privacy Act Reforms

Preparing for a new era in Australian Privacy

Privacy Act reforms: The *key* areas for change

Background for the reforms

Concluding four-years of industry and public consultation, Tranche 1 of the draft legislation for the *Privacy Act* Reforms ('PAR') was tabled in parliament in September 2024, covering the first portion of 116 proposals. The reforms, responding to shifts in public sentiment and notable data breaches, will introduce enhanced obligations relating to privacy that will significantly impact Australian organisations.

Significant new requirements*

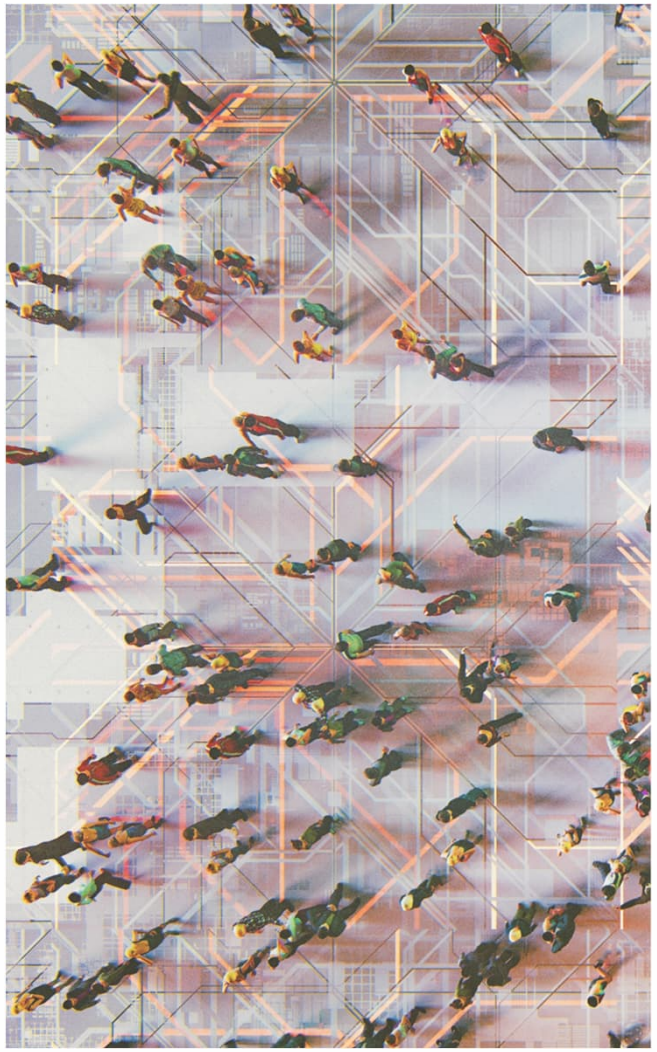
The reforms will require organisations to implement robust privacy governance and, in general, take a more proactive approach to privacy compliance. Tranche 1 of Draft Legislation includes: introduction of enhance security requirements; introduction of a Children's Online Privacy Code; mandated disclosures for use of Automated Decision Making; clarification of requirements for overseas data flows; new tiered penalties and infringements; and enhancement to eligible data breach responses.

Harmonisation with global legislation

The full-scope of the reforms are expected to bring Australia's privacy regime into alignment with existing global frameworks and other reforms – including the well-known GDPR, CCPA/CPRA and LGPD. Australia is one of the final jurisdictions to introduce comparable protections; this is good news for global organisations and those with mature privacy programs as they may already comply with elements of the proposed changes.

Strengthening regulator enforcement

In addition to introducing a number of improved investigation and enforcement powers to the OAIC (the regulator), the Privacy Commissioner has signaled a strategic shift to stronger 'outcome-based enforcement'. The enforcement-focused approach will see the OAIC aiming to "punch above its weight", in a manner that has been successful in achieving privacy-first outcomes (i.e. effective enforcement of privacy regulations) worldwide.



* The Attorney-General's Department has released Tranche 1 of Draft Legislation. The requirements outlined may change once finalised through Parliament and upon release of future Tranches of Draft Legislation.

Summary of *Draft Legislation*

Tabled to parliament on the 12th September 2024, the initial Tranche 1 of the Draft Legislation for the ongoing reforms included a total of 23 proposals, of the 116 initially proposed, covering the following key areas of the *Privacy Act 1988* (Cth).

Future Tranches

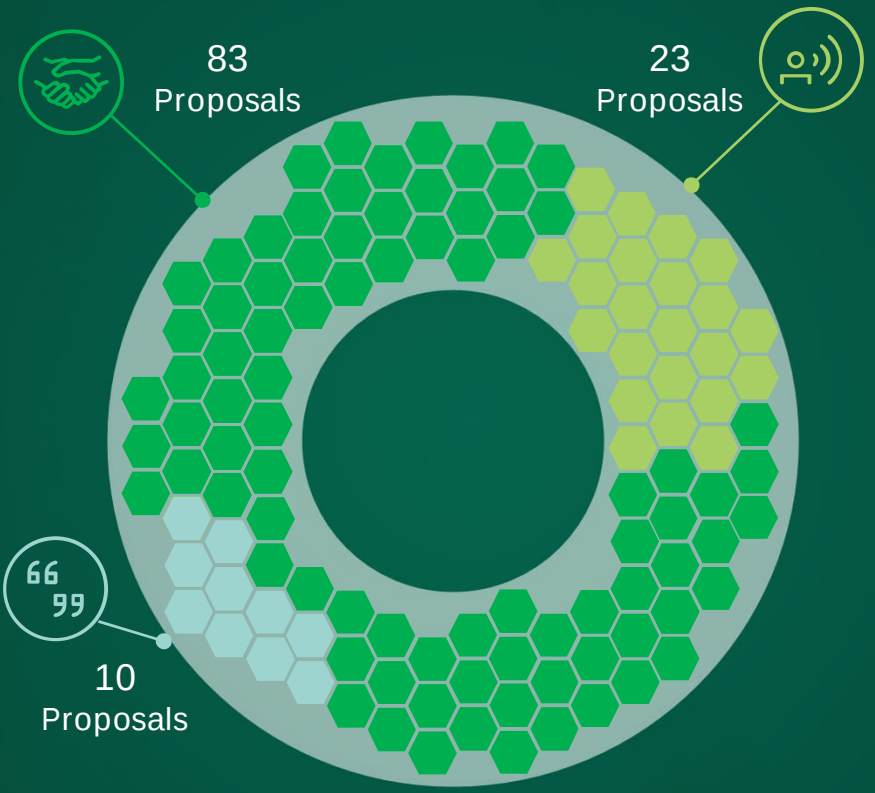
Proposals denoted as agreed-in-principle by the Australian Government (*September 2023*) and others not addressed within Tranche 1, which are expected to be subject to further refinement through industry engagement, impact analysis, and consideration around their interaction with related proposals.

Where practicable, organisations should begin to consider the impact of these being introduced.

Noted

Proposals denoted as 'noted' by the Australian Government (*September 2023*) that are unlikely to be progressed further.

These should still be *considered by organisations* to understand how they interact with related proposals and the other mechanisms that may be utilisied to respond to objectives and themes identified during the consultations.



Tranche 1

The following areas were introduced within Tranche 1 of Draft Legislation, and organisations should begin to prepare for these to be introduced:

- Children's Privacy: Development of a Children's Online Privacy Code for APP Entities handling children's personal information.
- Security of Personal Information: APP 11 to require organisations to implement technical *and* organisational measures to secure personal information.
- Overseas Data Flows: Clarification of APP 8 to allow for personal information to be shared with overseas entities where privacy laws/schemes are deemed to be 'substantially similar'.
- Eligible Data Breaches Declaration: The Attorney General enabled to declare an 'eligible data breach', specifying the personal information involved and permissible usage for reducing the risk of harm.
- New Penalty Tiers: Introduction of a tiered approach to penalties and infringement notices, for 'serious', 'not serious and 'administrative' breaches.
- Automated Decisions: Requiring organisations' to disclose in privacy policies if automated decisions utilise personal information, and the kinds of decisions made.

Australia's privacy pulse:

A snapshot of how people *feel*

Deloitte Australia's Privacy Index identified comprehensive consumer support for privacy reforms; a sentiment that has been motivated by the broad-impacts of notable data breaches and influence of global regulations.

Into the breach:
people's post-breach perceptions

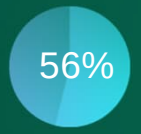
of consumers have been directly affected by a data breach in the past 12 months.

of those impacted felt vulnerable or angry.

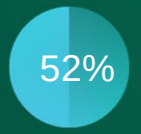
of people believe organisations should be held liable for compensating data breach victims individually for the potential harm and inconvenience.

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

The privacy pushback:
taking back control



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



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

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

of under 35-year-olds have chosen to leave a provider after experiencing a data breach.

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.

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.

Full Text: *Deloitte Australia 2023 Privacy Index*

Client perspectives: What we have *heard*

Sentiment from across the Australian public has driven into commercial spheres; with a desire to remain 'trusted' and ensure approaches to privacy reflect the expectations of their customers and employees.

"We are beginning to undertake impact assessments across the business, but the reforms are still uncertain"

"Our organisation is already aligned to the GDPR, we should be in a strong position"

"We are struggling to translate uplifts across different areas into a holistic program"

"We have started uplift initiatives, the change components will be challenging"

"There are certain areas of our organisation that will need to make drastic changes in order to remain compliant"

Understanding Impacts: Organisational *perspectives*

Privacy as a concept is broad and far-reaching. For this reason, the full scope of Privacy Act Reforms are anticipated to *impact many areas of an organisation*, not just legal and compliance. It will require engagement from functions tasked with information technology, security, and data; as well as sales, marketing and digital experience.

Legal and Compliance

The full scope of Privacy Act reforms are expected to introduce new requirements and challenges for legal and compliance functions. Organisations may be required to assign a senior employee with responsibility for privacy who will have a key role in ensuring compliance with privacy requirements. For serious breaches of privacy, organisations will face the heaviest fines yet - up to 30% of turnover. A renewed emphasis on organisational accountability will require proactive, robust privacy governance (including over their third-parties), requiring organisations to review how they write privacy policies, to make these easier to understand.

Who should care?

- *General Counsel/Legal Leadership*
- *Privacy Officer*
- *Chief Risk Officer*
- *Chief Compliance Officer*
- *Chief Procurement Officer*

Technology

New requirements within the reforms will mean changes to the ways in which technologies are designed and managed. Documented privacy risk assessments may be required when deploying major new systems and technologies. Security breaches may have to be notified to regulators within 72 hours, meaning implementation of new or enhanced incident response procedures. The Privacy Act reforms are expected to make Privacy Impact Assessments common practice across all areas of organisations over the next few years. In addition, organisations may be expected to look more into data masking, de-identification and encryption.

Who should care?

- *Chief Information Officer*
- *Chief Information Security Officer*
- *Chief Technology Officer*

Data

Individuals and teams tasked with information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what personal data is collected and where it is stored will make it easier to comply with new data subject rights - rights to have personal information erased and to be able to opt-out of specific processing activities. Organisations may be required to publish and enforce data retention periods.

Who should care?

- *Chief Data Officer*
- *Chief Operating Officer*
- *Chief Marketing Officer*
- *Data Stewards & Custodians*
- *Digital Leads*

Note: The Attorney-General's Department has released Tranche 1 of Draft Legislation covering some of the full 116 reform proposals. The requirements outlined may change once finalised through Parliament and upon release of future Tranches.

Organisational *perspectives:*
Legal and Compliance

General Counsels, Chief Compliance/Risk Officers, Chief Privacy Officers and Privacy Officers: Your privacy strategies, resourcing, and organisational controls will need to be revised. Boardrooms will need to be engaged more than ever before.

A Revolution in Enforcement

Fines of up to 30% of turnover during the breach period

'Serious' or 'repeated interferences' with privacy can now attract fines of up to 30% of turnover during the breach period, or $50 million (AUD) - whichever is greater.

Additionally, the OAIC will be provided powers to investigate and perform reviews into specific privacy matters; reducing the threshold for their interrogation on potential breaches, and supplementing their enforcement strategy.

Responsible Individual

Specialists in high demand

Organisations subject to the Australian Privacy Principles may be required to appoint or designate a senior employee with specific responsibility for privacy. This will present a challenge for many organisations, with privacy officers often holding a role in title, but not operationally. Organisations will need to ensure employees with responsibility for privacy are supported and can operate effectively.

Fair and Reasonable

Burden of proof on the organisation, not the individual

There may no longer the expectation on individuals to bear responsibility for whom they provide their data to – the introduction of an overarching 'fair and reasonable' test would shift the obligation for responsible and privacy-conscious data usage to organisations. To successfully operationalise, organisations would need to have effective privacy-assessment processes, and privacy-by-design processes.

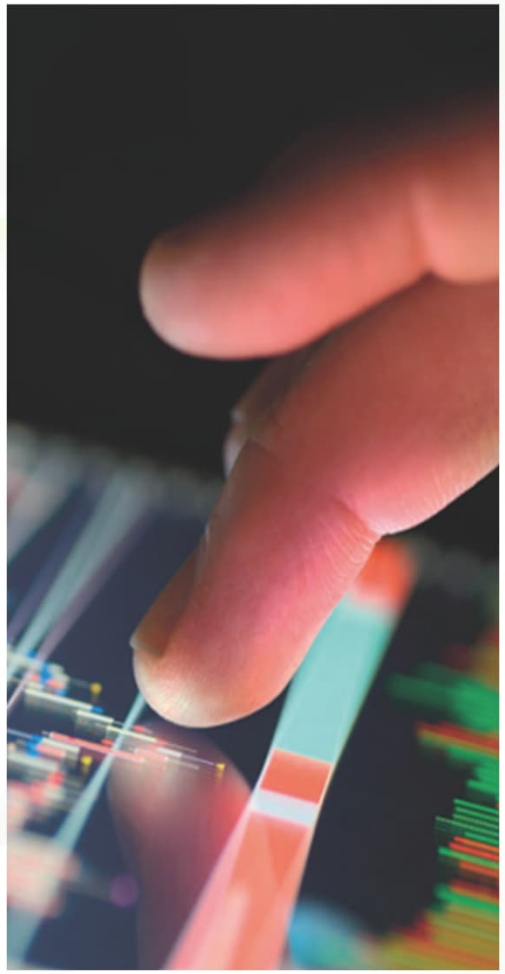
Privacy Notices and Transparency

Clarity and education is key

Organisations will need to carefully consider how they construct their privacy policies to provide more detail on specific topics (e.g. retention), and ensure they have external (public/customer facing) and internal (employee) coverage. It will no longer be good enough to hide behind pages of legalese, privacy policies must 'be clear and understandable'. Organisations may need additional consideration for privacy polices intended for children to ensure they can be understood.

Note: The Attorney-General's Department has released Tranche 1 of Draft Legislation. The requirements outlined may change once finalised through Parliament and upon release of future Tranches of Draft Legislation.

Organisational *perspectives:* Technology



Note: The Attorney-General's Department has released Tranche 1 of Draft Legislation. The requirements outlined may change once finalised through Parliament and upon release of future Tranches of Draft Legislation.

Chief Information Officers, Chief Technology Officers and Chief Information Security Officers: Your approach towards the use of technology to enable information security and other compliance initiatives will need to be reconsidered, with costs potentially rising.

Security of Personal Information

'Reasonable steps' to include technical and organisational measures

Organisations may be required to incorporate both technical (e.g. configurations, tooling) and organisational measures (e.g. training, processes), within the aspects of their security programs that cover personal information. This means organisations may have to urgently review and evaluate their end-to-end security mechanisms and processes to ensure adequate coverage.

Consent

Explicit consent now the 'norm'

The reforms would formally entrench the requirement that consent must be voluntary, informed, current, specific, and unambiguous. This would remove the ability to rely on implied consent and require organisations to not only consider the compliance components of how they collect, manage and trace consent, but additionally build this into their systems and platforms; this includes those external facing (e.g. websites and apps), and internal facing (e.g. data repositories, analytics platforms).

Online profiling and targeting

Limitations to online profiling and targeting

Enhanced requirements relating to the circumstances through which an individual can be marketed, targeted and profiled, would significantly impacting direct-to-consumer businesses who rely on such techniques to better understand their customers. This would apply not just to websites, but also to other digital assets, such as mobile applications, wearable devices, and current and emerging technologies.

Privacy-by-Design

Good practices required to meet accountability requirements

The concept of Privacy By Design (PbD) is nothing new, but would be an unavoidable requirement to enhance accountability. Requirements would mandate identification of the purpose and record of primary and secondary purposes collection and uses of personal information, and a requirement to mandate PIAs for all 'high-risk' activities (both technology and process related). Organisations would need to build a mindset that has privacy at the forefront of the design, build and deployment of new technologies.

Organisational *perspectives:*

Data

Chief Data Officers, Data Stewards, Chief Marketing Officers, and Digital Leads: Your information management activities have always supported privacy initiatives, but under the privacy reforms new activities are required which specifically link to compliance demands.

Data Inventories

Stronger need to identify and track personal information

Organisations would have to take steps to demonstrate they know what personal information they hold, the associated primary and secondary purposes, where it is stored, and who it is shared with, by creating and maintaining an inventory of processing activities. A thorough system for maintaining personal information inventories should be implemented, with specific consideration of retention periods – which will now be required to be disclosed.

Right to Erasure

A right for individuals to request deletion of their personal information

A proposed 'right to erasure' is further evidence of the consumer being in the driving seat when it comes to handling of their personal information. Organisations may be required to perform wholesale reviews of processes, system architecture, and third-party data access control to enable adherence to this right. In addition, archived data may also need to be reviewed and deleted.

Automated Decision Making (ADM)

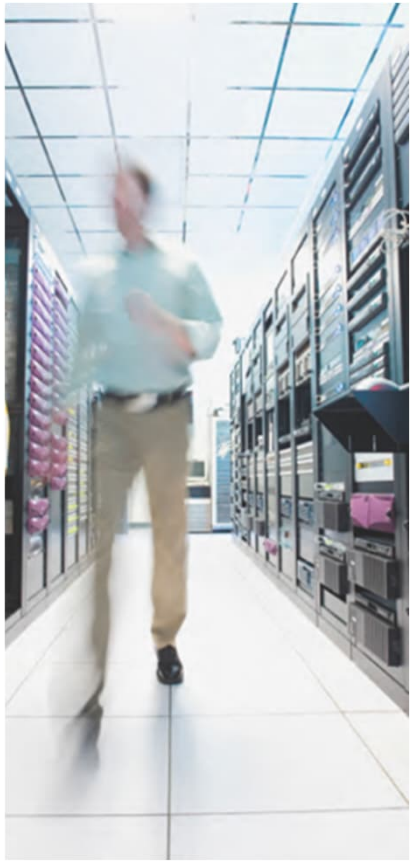
Scrutiny on the application of ADM, and the right to request information on ADM

Organisations may be required to disclose the types of personal information which will be used in 'substantially' automated decisions; alongside the introduction of a right for individuals to request meaningful information how automated decisions are made. This will require clear oversight and governance on ADM-related activities, and broader integration with a privacy program.

Expanded Definition of Personal Information

'Relates to' introduces a reduced threshold of identifiability

The reforms would expand the definition of personal information to cover that which simply 'relates to' an individual, placing a greater emphasis on information classification and governance. Previous ambiguity over certain data types, e.g. technical data, will be clarified to be within the expanded definition. This would remove ambiguity for unique or internal identifiers commonly used by organisations.



Note: The Attorney-General's Department has released Tranche 1 of Draft Legislation. The requirements outlined may change once finalised through Parliament and upon release of future Tranches of Draft Legislation.

Global privacy reforms: Lessons *learnt*

Deloitte Cyber has supported similar privacy reforms across Europe (GDPR), North America (CCPA/CPRA, CDPA etc.), South America (LGPD), and Asia (PDPA, PIPL, etc.). The following lessons were abstracted from our global privacy experts:

1. Awareness

The 'absorbent capacity' of a company is important in the implementation of organisational changes, including a privacy framework. Privacy awareness within the business is critical to support a successful transformation.

2. Buy-in

It is crucial to find the right leaders and people within your organisation to support and sponsor the implementation journey. They should cooperate and understand the need and the impact of the changes, both internally and with changing obligations.

3. Strategy and Assurance

It is important to develop a clear and achievable privacy strategy, supported by a risk-based approach to implementation and relevant controls, and control mechanisms. This should be deployed and monitored to understand the success of privacy reform initiatives and demonstrate accountability.

4. Change Management

In order to mature privacy capabilities, awareness and buy-in are a must have across first-line (business) teams. The associated communications, storytelling and storytellers are critical to ensuring effective change management.

5. Clarify Roles and Responsibilities

Where there are changes to controls, processes and existing practices, it is critical to ensure there is clarity over roles and responsibilities with respect to these changes; this may include the overarching operating model.

6. Tooling

When maturing your privacy program, tooling to support specific capabilities (data mapping, customer requests, consent and preference management, TPRM) should be implemented. They provide improved visibility, allowing for proactive management and strategic decision-making regarding privacy.

Practical steps to Privacy Act compliance: Building a *change* program

A combination of both tactical and strategic actions will be required to achieve compliance with the *Privacy Act*, often over a period of months and years. The below elements are expected to be required to drive organisational and cultural change and embed the full scope of Reform requirements into business as usual.

FOUNDATIONAL ACTIVITIES

Stakeholder Awareness – Ensuring stakeholders are aware of the upcoming reforms, their scope and impacts.

Readiness Assessments – Understanding where your organisation may need to invest in resourcing and/ or financially to prepare.

NO REGRETS

Data Inventories and Mapping – Compile an inventory of the PI collected, information flows, who it is shared with and what controls govern its use and disclosure.

Governance and Operating Model - Assess your holistic approach to privacy governance, and the overarching privacy operating model.

1

CUSTOMER & EMPLOYEES

Employee or Customer Journeys/Data Flows – Discover and document customer journeys/data flows, and ensure individuals are provided clear and transparent disclosures at the point of collection/intake.

Right to Access, Right to Correction, Right to Erasure – Develop processes to promptly triage, validate and respond to data access, correction, erasure requests.

Consent, Trading & Right to Opt-out – Review and update consent mechanisms and preferences, including downstream flows through the organisation for other processing purposes and sharing.

2

Identity Consolidation & Uplift – Review and enhance customer identity consolidation and management approaches, across customer profiles and first-party data.

SECURITY

4

Breach Management & Notification Procedures – Review existing breach management processes and associated notification procedures; ensure they are documented, well-understood and thoroughly tested.

Technical & Organisational Measures – Collaborate with security capabilities to review the availability and implementation of technical measures across personal information processing and storage (e.g. encryption, access controls); assess organisational measures (e.g. incident response plans, security training).

Third-Party Management (Vendors & Suppliers) – Review contracts and agreements with third-parties; remediate or re-negotiate contracts where required; enhance monitoring and off-boarding for third-parties.

Overseas Transfers – Identify and review all overseas transfers of personal information, remediate where no-longer permitted and update required disclosures.

DATA LIFECYCLE & MANAGEMENT

3

'Fair and Reasonable' Test – Review existing and new processing of personal information to ensure all meet the standard of 'fair and reasonable';

Privacy Impact Assessments – Ensure PIA processes, triggers and questionnaires are established; perform a PIA over any existing personal information processing.

Automated Decision Making – Identify all circumstances of ADM, review the types of decisions and information utilised, and integrate required disclosures into transparency measures and disclosures (e.g. privacy policies).

Retention Tooling & Triggers – Review defined retention periods, implement or update retention triggers, and integrate required disclosures into transparency measures and disclosures (e.g. privacy policies).

Destruction & De-identification – Continue, or commence, activities to destroy or de-identify information that is no longer needed.

Why Deloitte:
Our *global* experts

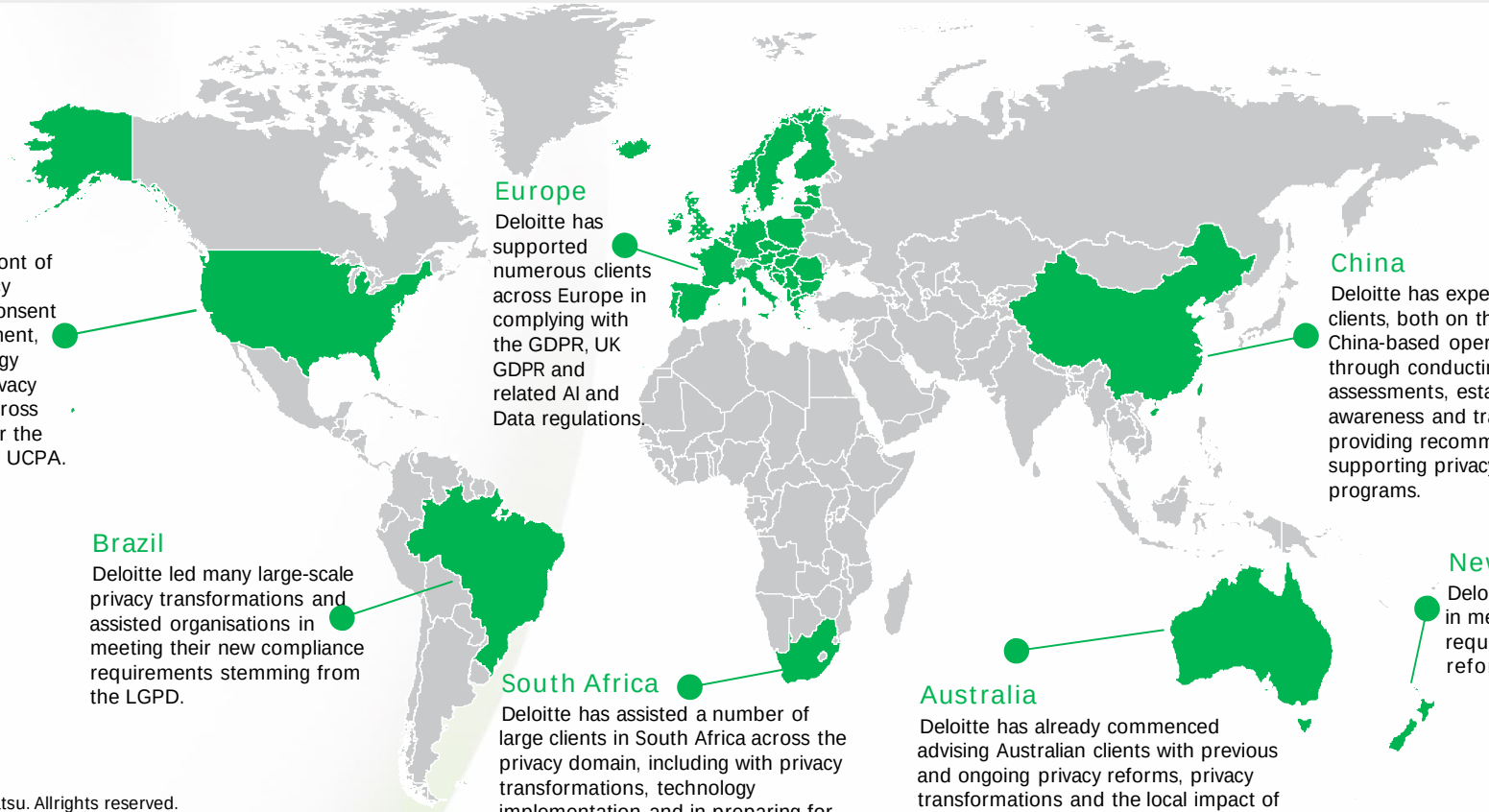
Deloitte has global professional network, and we have provided support with privacy reforms across all continents over recent years. Our global experts are ready to support Australian reforms where appropriate, through their expertise and learned experience.

21,000+ cyber and privacy professionals worldwide

1,000+ privacy professionals worldwide

150+ offices across APAC and Globally

25+ years providing cyber and privacy risk services



United States
Deloitte was at the forefront of providing specialist privacy services encompassing consent and preference management, privacy enabling technology implementations, and privacy program development across S&P 500 organisations for the CCPA/CPRA, VCDPA and UCPA.

Europe
Deloitte has supported numerous clients across Europe in complying with the GDPR, UK GDPR and related AI and Data regulations.

China
Deloitte has experience preparing clients, both on the mainland and with China-based operations, for the PIPL through conducting maturity assessments, establishing data privacy awareness and training programs and providing recommendations and supporting privacy remediation programs.

Brazil
Deloitte led many large-scale privacy transformations and assisted organisations in meeting their new compliance requirements stemming from the LGPD.

New Zealand
Deloitte has assisted clients first-hand in meeting their enhanced compliance requirements stemming from the 2020 reforms to the Privacy Act.

South Africa
Deloitte has assisted a number of large clients in South Africa across the privacy domain, including with privacy transformations, technology implementation and in preparing for and complying with the POPIA.

Australia
Deloitte has already commenced advising Australian clients with previous and ongoing privacy reforms, privacy transformations and the local impact of global privacy reforms.

Why Deloitte:
Our *alliance* partners

Deloitte has strategic and global alliances with industry recognised partners to develop, deploy and operate their market leading capabilities and address complex privacy-related issues that no single organisation can solve themselves.

OneTrust Global Strategic Partner

OneTrust is an industry leading tool, covering privacy governance and assessment automation, consent and preference management, data discovery, record of processing, compliance automation, third-party management and AI governance.

Deloitte has a global capability, including in Australia, with over 150+ OneTrust certified professionals.

Adobe Global Alliance Partner

Ranked as a leader in global digital experience platforms *(Gartner, 2024*), Adobe's Experience Platform provides capabilities across analytics, customer journeys and customer data.

Adobe's Real-Time CDP integrates with OneTrust Consent & Preference Management to provide privacy-first personalisation and segmentation.

Salesforce Global Alliance Partner

Salesforce provides integrated capabilities across customer data, channel and preference/consent management.

This can be supported by centralised privacy management, with separate capabilities for customer case management for individual rights requests, privacy-related complaints and inquiries.

ServiceNow Global Alliance Partner

ServiceNow is a global leader in governance, risk and compliance (GRC) tooling, with specific tooling capabilities in both Security Incident Response and Privacy Management.

This includes privacy assessments and risk management, third-parties/vendors, records of processing, control testing automation and privacy case management.

Ping Global Alliance Partner
Okta Implementation Partner

Capture, storage and enforcement of customer and employee consent (with optional OneTrust integration), identity validation and authentication, and customer identity management (including update and erasure).

Deloitte was awarded the OKTA Global System Integrator Partner of the Year (2023).

SAP Global Alliance Partner

As a global leader in ERP/HCM applications and business AI (*Gartner, 2023*), SAP stands at the nexus of business and technology.

SAP solutions offer specific features to support adherence to enhanced privacy obligations under the reforms, including: retention and destruction, classification, consent, individual rights and personal information security.

Tealium Implementation Partner

Ranked a leader in global customer data platforms *(Gartner, 2024),* Tealium offers intrinsic capabilities for customer consent and preference management, cookie consent and opt-out.

Tealium allows for direct integration into activation and data platforms, and a consent register (for consent status sharing).

Securiti Implementation Partner

Offering capabilities in: privacy management (assessment and breach); data discovery and mapping; privacy policy and notice management; consent; consumer privacy centre; and individual rights automation.

Securiti was named a leader in global privacy management platforms *(Gartner, 2024).*

How we can support you:
Our *privacy* services

We have a dedicated team of privacy and cyber security specialists, with deep expertise in leading privacy programs across complex and global organisations, embedding change, and supporting privacy *advisory*, *implementation* and *operate* capabilities.

Our team performed an assessment of a large technology organisation's readiness with proposed Privacy Act reforms requirements, issuing a formal report and prioritised compliance roadmap

We designed and established a new privacy function for an Australian Conglomerate, creating a governance model, policies and processes and bespoke privacy training

We designed and implemented a group wide privacy program for a consumer business client, and delivered a gap analysis, a PIA procedure, policies and privacy operating model

We supported the cyber response for a consumer business client which had suffered hacking and a data breach, providing advice on their customer notification and regulatory obligations

Compliance and Readiness	Privacy Programs	Technology and Digital	Risk Management	Training and Cultural Change	Cyber Security	Consent & Identity
• Privacy maturity and readiness assessment • Privacy compliance roadmap • Global privacy compliance assessments • Privacy technology impact assessment	• Privacy program development • Privacy strategy and roadmap development • Target operating model design and implementation • Change program design and delivery • Individual Rights Strategy, Approach and Processes • Secondments & Virtual Privacy Office	• Data discovery, mapping and inventories • Privacy Governance Tooling • Privacy-by-design advice and application • Spam Act and marketing reviews • Privacy Enhancing Technologies (*PETs*) • Data Privacy Management Technology Implementation • Data Retention & Destruction strategy and operationalisation	• Privacy Impact Assessments (*PIAs*) • PIAaaS (*Operate Capability*) • Policy analysis and design • Governance and compliance review • Third party management • M&A due diligence, data transfer and ownership support	• Privacy risk and compliance training • Training and awareness design and implementation • Classroom and computer bases training • Cultural change programme development	• Personal data breach investigation and management • Regulatory liaison advice • Incident response and forensic investigation support • Supplier and third-party management • Data Breach Response as a Service (*Operate Capability*)	• Consent Strategy & Approach • Consent CX/UX and Customer Journey Mapping • Consent and Preference Management tooling • Customer Identity and Access Management (CIAM) • End-to-end Customer Identity Solutions • Identity Verification and Validation • Individual Rights Tooling

 |

Getting on the front foot:

A conversation *today*, to set you up for *tomorrow*

Get in touch now

Daniella Kafouris
Partner | Cyber, Technology & Transformation
dakafouris@deloitte.com.au
+61 3 9671 7658

Lucy Mannering
Partner | Cyber, Technology & Transformation
lmannering@deloitte.com.au
+61 2 9322 7645

Jarrod Oakley
Partner | Cyber, Technology & Transformation
jaoakley@deloitte.com.au
+61 3 9671 7267

Kate Monckton
Partner | Cyber, Technology & Transformation
kmonckton@deloitte.com.au
+61 2 8260 6059

Piya Shedden
Director | Cyber, Technology & Transformation
pishedden@deloitte.com.au
+61 407 854 187

Tim Scott
Director | Cyber, Technology & Transformation
timscott@deloitte.com.au
+61 407 930 611

Marie Chami
Director | Cyber, Technology & Transformation
mchami@deloitte.com.au
+61 431 239 486