



Risk in Super Series
Privacy and the future of Member ID

15 June 2023

Keynote Speaker



Athena Efstratiadis

Head of Compliance, REST

Deloitte Insights



Lucy Mannering

Partner, Risk Advisory
Cyber and Strategic Risk



Cheryl Cheong

Partner, Risk Advisory
Regulatory and Compliance Risk



Natalie Reed

Director, Risk Advisory
Digital Identity

Proposed Changes to the Australian Privacy Act

On 16 February 2023, the Attorney-General's Department released their *Privacy Act Review Report*, containing 116 proposals to strengthen Australia's *Privacy Act 1988* (Cth) (Privacy Act). The below provides a snapshot of 10 key proposed changes which are likely to have significant impact on a superannuation fund. The proposed changes represent a continuation in the uplift of the current Australian privacy law framework and a greater alignment with global privacy laws.

1. Expanded definition of personal information



6. Shorter timeframe for data breach notification



2. Strengthened consent requirements



7. Clarified definition and protections for de-identification



3. Enhanced protection for employee personal information



8. Additional rights and protections for marketing and targeting



4. Introduction to new individual rights



9. Introduction of a 'fair and reasonable' test



5. Strengthened controls for overseas data flows



10. Transparency and review of retention periods



What do the proposed changes mean for your organisation?

There are 10 key proposals in the new Privacy Framework which are likely to have considerable impact on a super fund's day-to-day operations.



1. Expanded definition of personal information

How can you prepare?

- **Undertake a data mapping exercise** to identify all personal information held by your organisation including additional information that will fall under the expanded definition.
- **Review and update the privacy framework** including all supporting processes, procedures and documentation to extend existing privacy protections to new information types, to ensure it is protected and destroyed when no longer required.
- **Communicate and educate technical, data and customer facing staff** on the expanded definition through training and awareness.



2. Strengthened consent requirements

How can you prepare?

- **Move to a privacy-by-default model for all online privacy settings.** For example, do not use bundled consent or pre-ticked boxes to collect consent as these may not meet the new proposed conditions for consent.
- **Review how consent is currently obtained** and consider how more meaningful consent can be collected from individuals.
- **Develop and test consent withdrawal processes** to determine whether they would meet the proposed requirement for being as easy as the provision of consent.



3. Enhanced protection for employee personal information

How can you prepare?

- **Consider whether any existing personal information processes can be leveraged** for the protection of employee personal information and if any new processes need to be developed (e.g., a procedure for handling employee personal information, data mapping of employee information).
- **Determine how enhanced transparency can be provided to employees** regarding the collection and use of their personal information (e.g., through review/uplift of privacy policies).
- **Update data breach response plan** to include employee personal information.



4. Introduction to new individual rights

How can you prepare?

- **Understand where all personal information in the business resides** (e.g., through data mapping and development of a register of personal information processing activities).
- **Update individual rights processes and procedures** to cover requirements for new and amended individual rights and to ensure that they can be fulfilled within 30 days.
- **Train all relevant staff on what individual rights are** and how to fulfil an individual rights request.



5. Strengthened controls for overseas data flows

How can you prepare?

- **Identify and document all data flows with third parties and interorganisational data flows outside of Australia.**
- **Review controls for sharing personal information with third parties and consider how these can be strengthened** (e.g., check that a contract exists with third parties to govern all international transfers of personal information).

What do the proposed changes mean for your organisation?

There are 10 key proposals in the new Privacy Framework which are likely to have considerable impact on a super fund's day-to-day business operations.



6. Shorter timeframe for data breach notification

How can you prepare?

- **Review and uplift data breach response plan** and processes to allow for the identification and reporting of eligible data breaches to the OAIC within a 72 hour window.
- **Update and test data breach response plans** and processes through simulations and/or table top exercises and amend as required.
- **Train staff on what constitutes a data breach** and the process for reporting one.



7. Clarified definition and protections for de-identification

How can you prepare?

- **Identify all de-identified data sets held** and assess whether they can still be considered as de-identified under the proposed definition. This should include an assessment of the re-identification risk.
- **Consider removal of de-identified data sets** that are no longer required, and which are at risk of re-identification.
- **Consider how current security and overseas disclosure requirements and controls can be extended** to de-identified data sets.
- **Review de-identification techniques and assess whether they are still fit for purpose** or if they need to be strengthened.



8. Additional rights and protections for marketing and targeting

How can you prepare?

- **Review all direct marketing and targeted advertising activities** and consider limiting, amending or ceasing activities that do not align with the proposed requirements and with the expectations of the individual.
- **Review all direct marketing and targeted advertising activities directed at children**, assess whether these activities are in the best interest of the child and cease activities that are not in their best interest.
- **Develop an opt-out method for targeted advertising** and ensure that it meets the requirements for withdrawing consent as easily as providing the consent.



9. Introduction of a 'fair and reasonable' test

How can you prepare?

- **Review existing personal information uses** in line with the 'fair and reasonable' test and remediate where activities do not align with the test.
- **Document the fair and reasonable test** prior to processing personal information for any new uses to demonstrate it has been considered.
- **Review privacy policies, collection notices and consent** and consider how they meet the fair and reasonable test, in particular, transparency and appropriate collection and use.



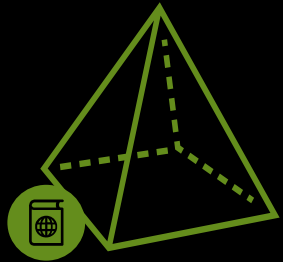
10. Transparency and review of retention periods

How can you prepare?

- **Review retention schedule and associated records management policies** and define minimum and maximum retention periods, considering legal and business requirements for retention.
- **Update privacy policies to include specified minimum and maximum retention periods** for personal information.
- **Review personal information retained against the retention periods defined** and conduct remediation of any records that are no longer required.

Identity Trends Overview

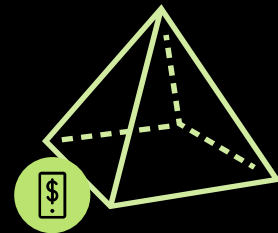
A shift to digital has reduced the robustness of the identity assurance process and the ability to rely on this data in isolation.



KYC processes emerged from the 100 point check which is a pre-digital world process



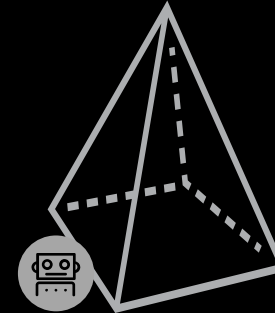
Physical possession was key



Seismic shift to digital services



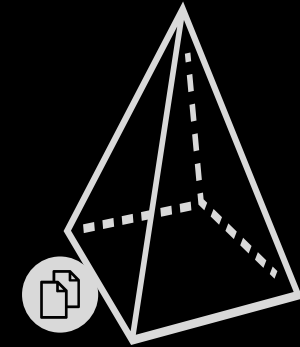
No comparable rethink of physical equivalence



Significant degradation in identity assurance



Reliance on identifiers which are simply data



Identifiers can be shared and copied



Identifiers proliferate on the dark web

The Challenge:

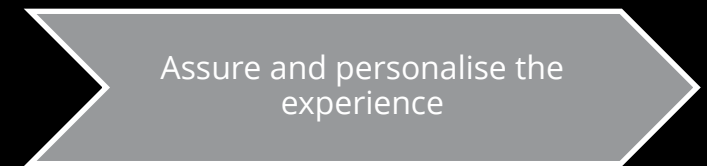
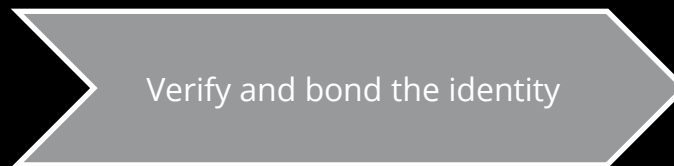
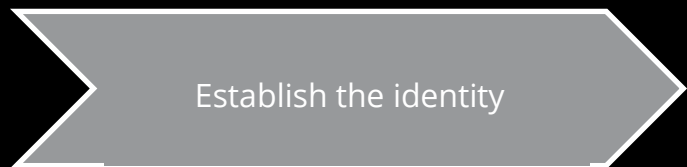
How can we better bind the physical identity to those identifiers that are used in a digital environment?

Identity Trends Overview

It is critical now more than ever before to think about how members move safely and seamlessly through the onboarding journey...

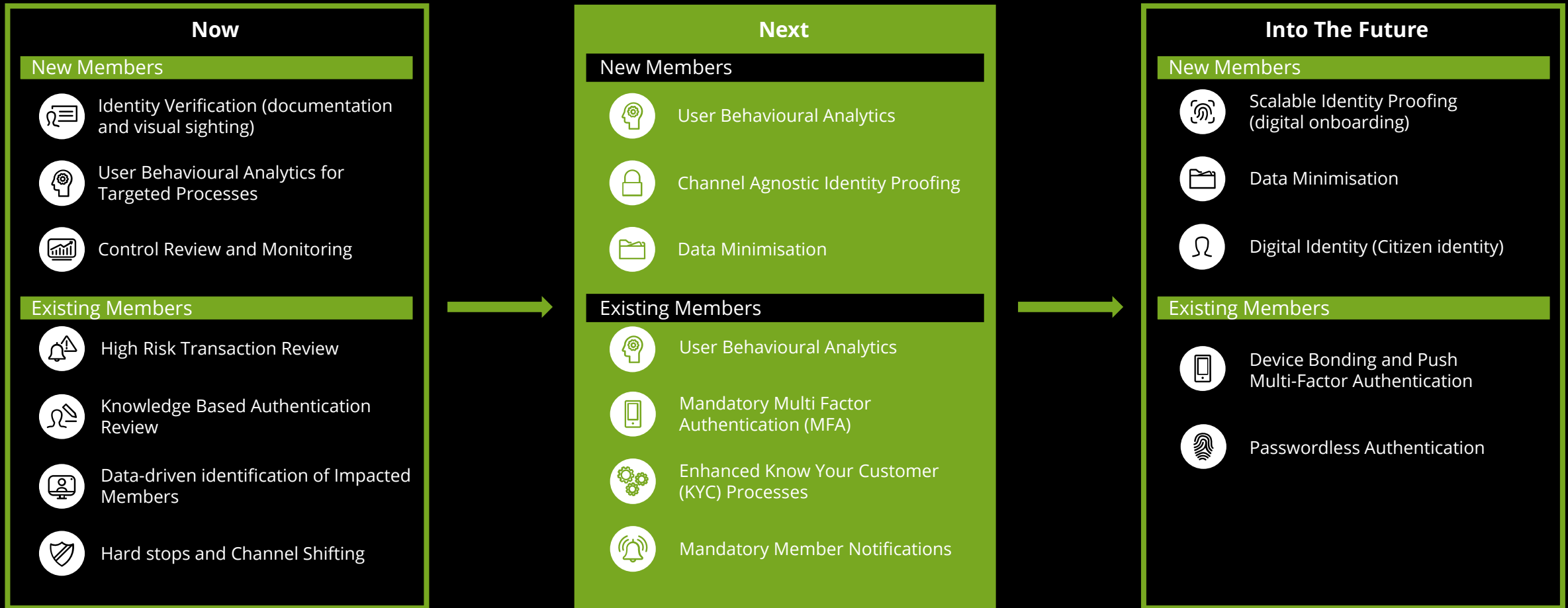


- User Behavioural Analytics
- Traditional Identity Proofing
- Document Scanning (using facial recognition to verify the data, document and face)
- Biometric Bonding for trusted devices
- Verified attributes (such as phone number and email)
- Strong Authentication, using Multi-factor Authentication
- Trusted Devices
- Risk-based Interaction Controls
- Event-based customer notification



Mitigation – Short, Medium and Long-Term Considerations




Considerations to overcome the challenges that will be faced by your fund now, and into the future.



Why managing data risk is important to the super industry

As organisations put data to use strategically as a business asset in increasingly complex and innovative ways, and regulatory and public scrutiny of data practices continues to mature, building trust in data is a business imperative

Momentum has been building behind the key drivers of data risk

-  Digital and AI-driven transformation is increasing the scale and complexity of the data eco-system
-  Data *innovators* and *predators* are driving disruption and competition for incumbents
-  Regulation and regulatory scrutiny of data practices is maturing
-  Members and other stakeholders expect data will be safe
-  The data quality challenge is persistent and is becoming more transparent to stakeholders
-  The scope, granularity and complexity of regulatory data collections is expanding
-  Organisations expect their data capability investments will generate a return



We see the impact of data risks playing out across six domains

Competitive Advantage

Margin loss and not being able to compete through new products, services, channels and technology

Member Outcomes

Poor member experience, unsuitable products/services and not meeting data use expectations

Cost of Ownership

Inability to control costs due to ineffective coordination of data investment or proliferation of data debt

Compliance

Failure to demonstrate that data is managed sufficiently to satisfy regulatory scrutiny and regulatory and legal obligations

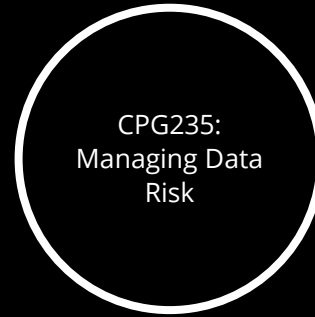
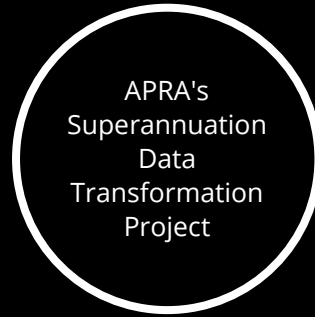
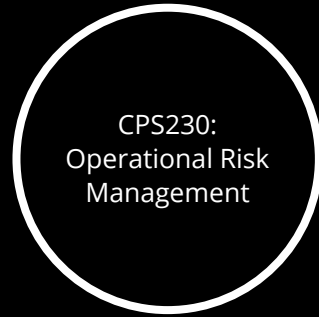
Governance

The risk that data isn't managed such that it is understood, trustworthy, fit-for-purpose and available

Decision Making

Impact on decision making which may be inefficient or ineffective due to untrustworthy data

Data risk regulatory and compliance drivers



What does this mean for Superannuation Funds?

Data Governance

Demonstration of strong governance, including senior management and Board oversight of data.

Clearly defined roles and responsibilities.

Data Risk

Adopting a systematic and formalised approach to data risk management, identifying and mitigating risks throughout the data lifecycle including business continuity.

Operationalisation and assurance are key components, regular assessments to measure and ensure ongoing effectiveness of data risk and the control environment.

Data Quality

Being able to assess and manage its data quality through clear framework/processes to identify, resolve & report data quality issues.

Data Controls

Adopting a risk-based approach which designs and implements data controls and regularly assesses the operational effectiveness of the controls (commensurate with the size, business mix and complexity of the activities they undertake) to ensure that data requirements are met at all stages of the lifecycle.

What are the benefits?

Enables an organisation to manage its data as an asset, ensuring data accuracy, consistency and reliability, reducing and mitigating risks and improving the ability to respond to regulatory requirements.

Effective management of data risk reduces the likelihood of loss or failure to meet business objectives, and/or loss of the value associated with data.

High quality, reliable and trustworthy data helps organisation's realise and potentially increase the value of its data, as well as reducing risk associated with poor quality data.

Supports the organisation's operational risk, improves decision making and planning, and offers operational efficiencies in being able to enhance responsiveness and resiliency.

Industry data risk focus areas

Based on our experience with clients within the financial services and insurance industry, there are 4 key focus areas which super funds also need to consider.



RISK APPETITE

Data risk appetite must be defined at enterprise and division/BU levels, including tolerance levels for key risk indicators (KRIs). Divisions/BUs ultimately own the data risk and therefore need to drive the definition, management and monitoring of appetite statements, tolerances and indicators.



DATA RISK PROFILE

Undertaking data lineage and value chain exercises including determining if any of the assessed material data risk could manifest, identifying a control (or set of controls) for each risk and consideration for how the data is being used downstream. Data controls need to be recorded in the same GRC system as other material risks and assessed for effectiveness.



THIRD & FOURTH PARTY RISK

Organisations must identify, assess, manage outsourced service providers, identify material service providers that enable critical operations or expose the organisation to material operational risks.



ALIGNMENT OF DATA AND TECHNOLOGY STRATEGIES

Dependencies and linkages between data and technology strategies are understood and explored. Evidence of embedding the data management and architecture principles in the target state design decisions and overarching environments.

Panellist Q&A

Key Contacts



Lucy Mannering

Partner, Risk Advisory
Cyber and Strategic Risk
lmannering@deloitte.com.au



Cheryl Cheong

Partner, Risk Advisory
Regulatory and Compliance Risk
chercheong@deloitte.com.au



Melissa Gomes

Partner, Risk Advisory
Financial Industry Risk and Regulation
melgomes@deloitte.com.au



Natalie Reed

Director, Risk Advisory
Digital Identity
nareed.@deloitte.com.au



Jaramie Nejal

Director, Risk Advisory
Financial Industry Risk and Regulation
jnejal.@deloitte.com.au



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. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

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.

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 416,000 people make an impact that matters at www.deloitte.com.

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.

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 8000 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.