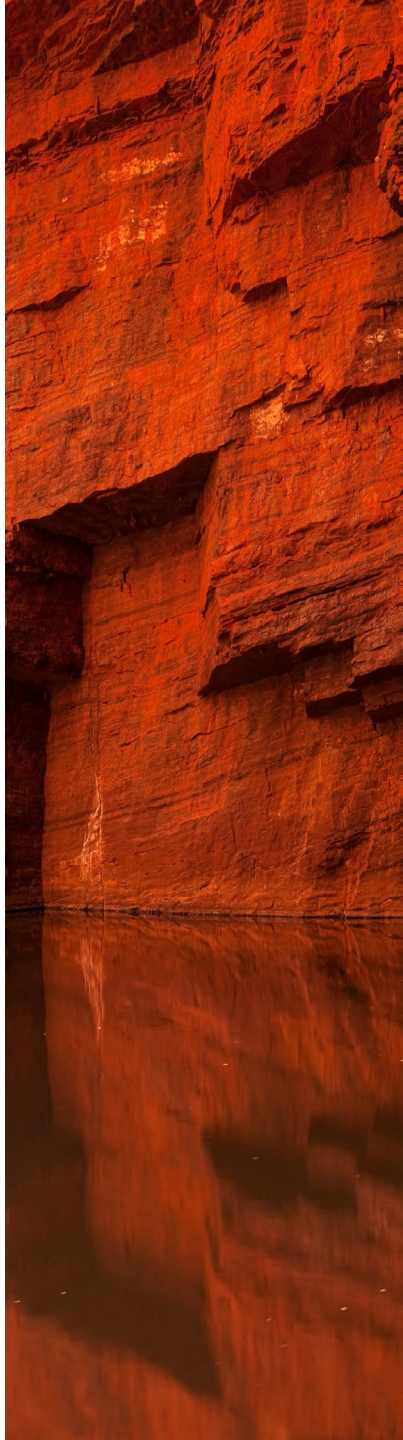
# PRIVACY LAW AND ITS APPLICATION TO SSOs

*NSW Office of Sport*
*SSO Professional Development Webinar*

**Simon Merritt, Special Counsel**

**25 October 2023**

LANDER & ROGERS



# ROADMAP

- Why is protecting privacy important?
- Privacy law basics
- Mandatory data breach notification regime
- Consequences of non-compliance
- SSO-specific scenarios

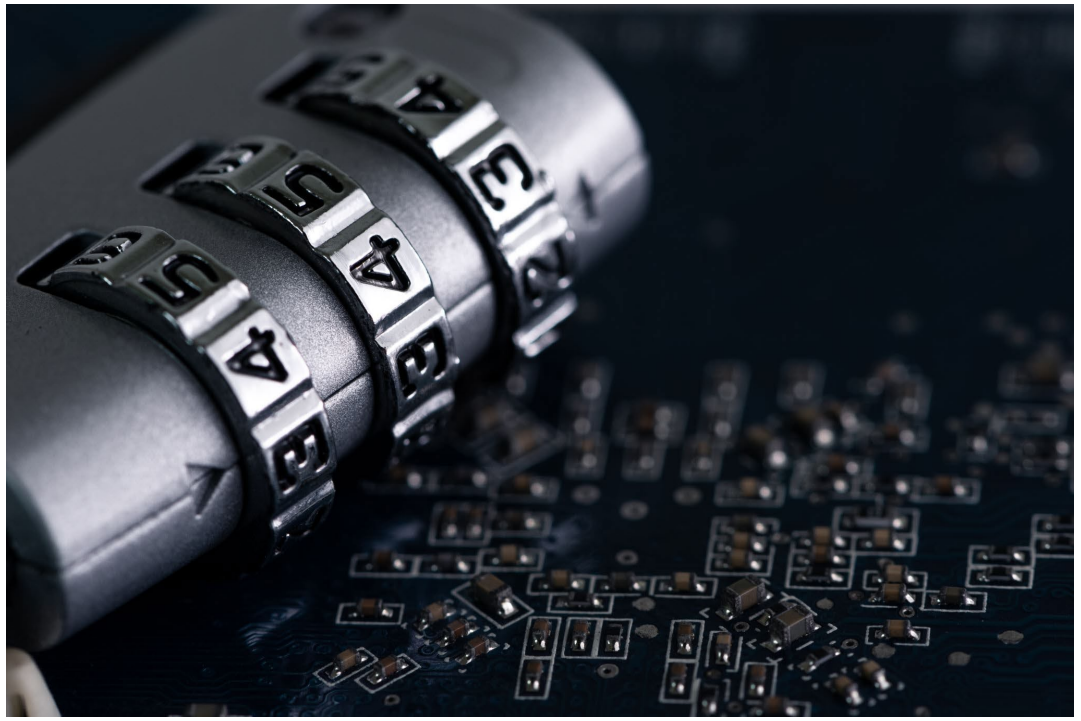
LANDER & ROGERS

# WHY IS PROTECTING PRIVACY IMPORTANT?

- Individuals care about interference with their privacy and data breaches
- New technologies – sophisticated technology, delivery of products through apps, rapid and free flowing sharing of personal information and social media trends
- Reputational damage for poor handling of personal information
  - E.g. Optus, Medibank

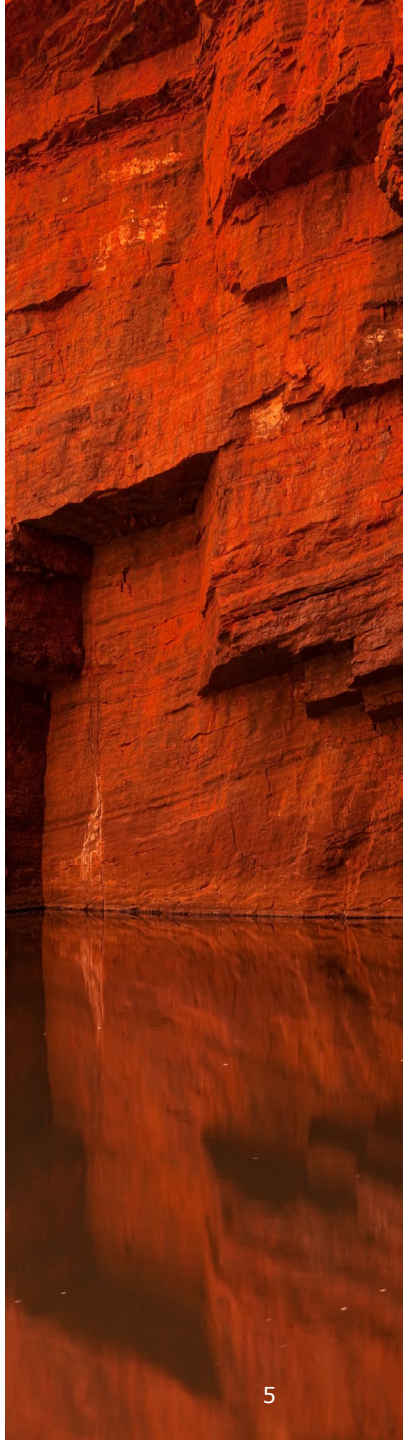
# Privacy Act Review Report – Government Response

- Potentially major changes
- In-principle agreement to key matters
- Relevant to SSOs:
  - Removal of small business exemption
  - Change to or removal of employee records exemption
  - Consent definition – voluntary, informed, current, specific and unambiguous
  - Express ability to withdraw consent
  - Right to erasure, right to object to collection



# PRIVACY LAW BASICS

- Who is bound by the Privacy Act?
- What is personal information?
- Australian Privacy Principles
  - Part 1 – Consideration of personal information privacy (eg, privacy policies)
  - Part 2 – Collection of personal information (eg, solicited and unsolicited personal information)
  - Part 3 – Dealing with personal information (eg, use or disclosure, direct marketing, cross-border disclosure)
  - Part 4 – Integrity of personal information (eg, quality and security of personal information)
  - Part 5 – Access to, and correction of, personal information

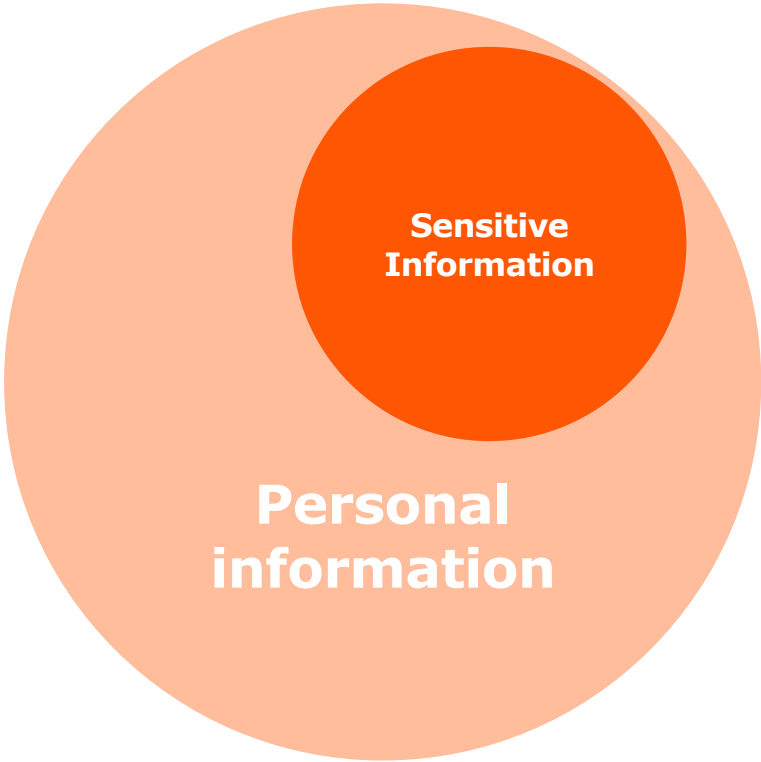


# WHO IS BOUND BY THE PRIVACY ACT?

- All "**APP entities**" are bound by the Privacy Act
- An "APP entity" is defined to be an agency or organisation
  - ***Agency*** – Australian Government agencies but does not include State and Territory agencies.
  - ***Organisation*** – An individual (including a sole trader), a body corporate, a partnership, any other unincorporated association, or a trust unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State
- **Exempt: "Small business operator"**
  - Organisations with an annual turnover of $3 million or less for a financial year are exempt

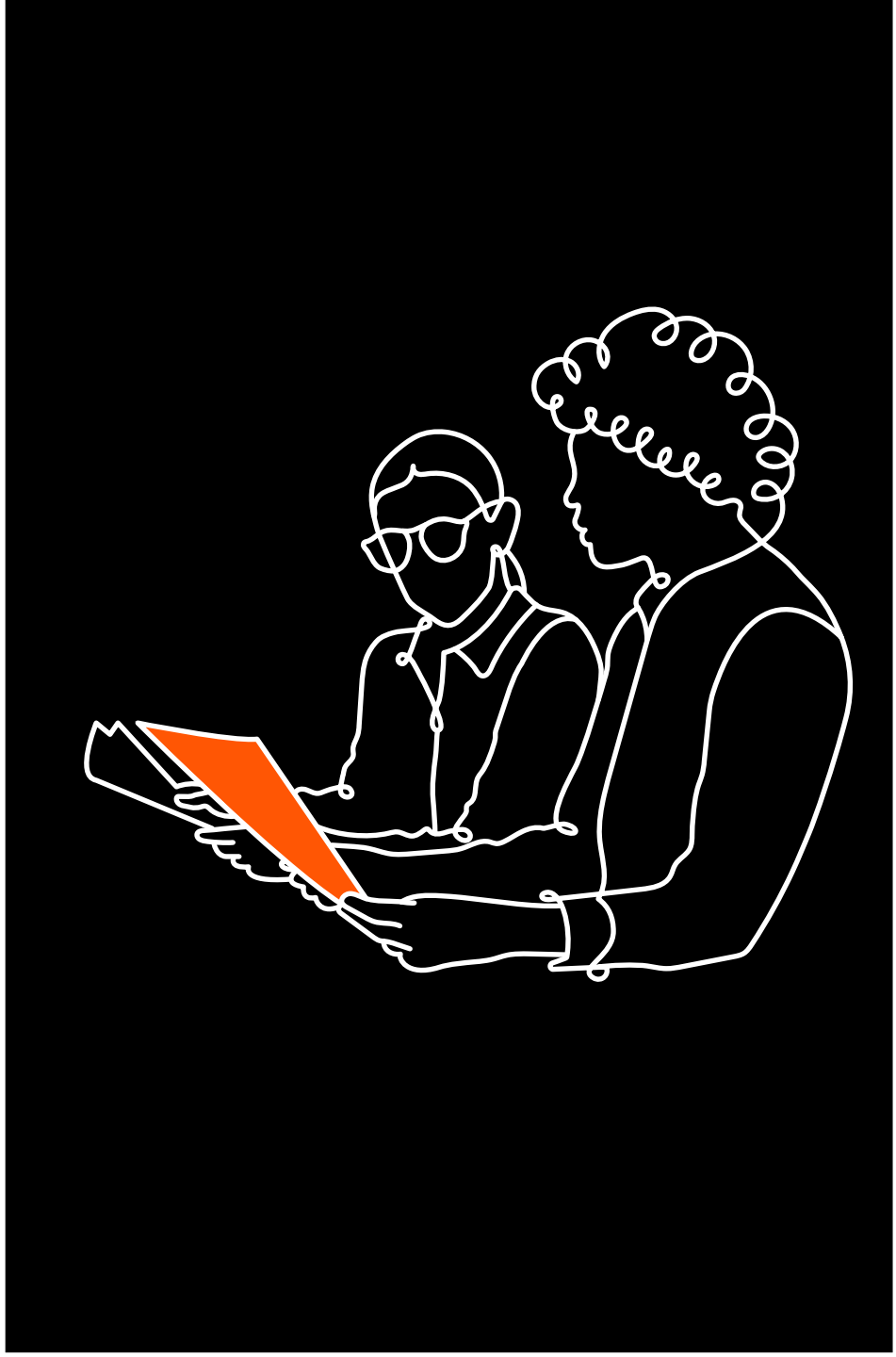
# WHAT IS PERSONAL INFORMATION?

- **Personal information**
  - Information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not
- **Sensitive information**
  - Subset of personal information
  - Eg, Racial origin, health information, political opinion, criminal records
- **Exempt information: employee records**



# EMPLOYEE RECORDS

- Exemption from Privacy Act requirements
- APPs can be followed for risk management
- Employee requests for records under workplace legislation



# PROSPECTIVE EMPLOYEE INFORMATION AND CONTRACTORS

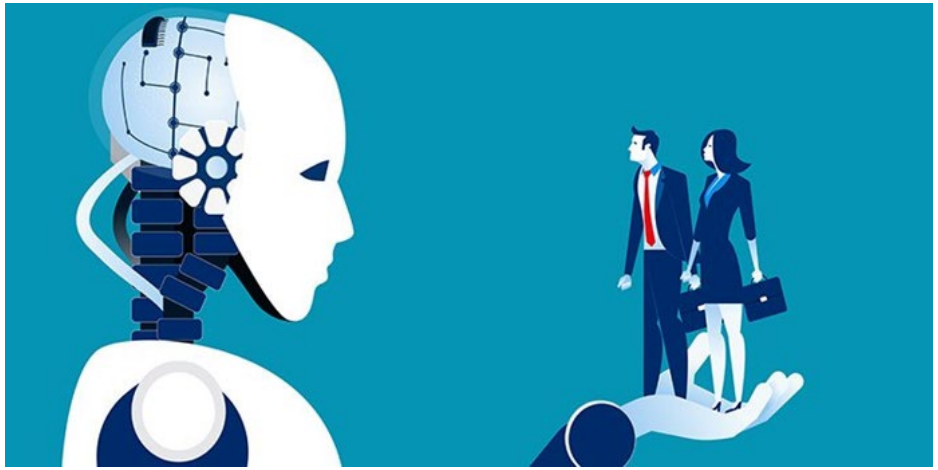

- Employment relationship
- Unsolicited CVs
- Pre-employment checks (background, reference and medical checks)

## Privacy Policy

- APP 1.2 – APP entities must have a clearly expressed and up-to-date privacy policy which sets out how the entity will manage the personal information collected by it
- The information which must be in a privacy policy is:
  - **Types of personal information collected**
  - **How the info is collected and used**
  - **Why it is collected, used and disclosed**
  - **How individuals can access and correct their information**
  - **Complaint procedures**
  - **List of overseas countries where info may be disclosed**

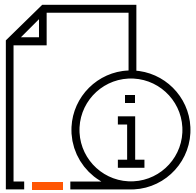
# Collection of personal information

- APP 3.1 and 3.2 – APP entities must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities
- APP 3.3 – Sensitive information must not be collected unless the individual has consented to the collection
- APP 3.6 – Personal information must only be collected from the individual unless it is unreasonable or impracticable to do so



# AUSTRALIAN PRIVACY PRINCIPLES (OVERVIEW)

## Notification of collection of personal information



- APP 5.1 – Where an organisation collects personal information about an individual, the entity must notify the individual about specific matters (known as a "collection notice")
- APP 5.2 – Matters to be addressed in a collection notice include: the organisation's identity and contact details, circumstances of collection, purpose(s) of collection, information about access and correction & complaints process, list of overseas countries where likely to be disclosed

## Use and disclosure

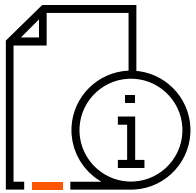
- APP 6.1 – If information was collected for a particular purpose (primary purpose), the entity must not use or disclose the information for another purpose (secondary purpose) unless an exception applies.

# WENTWORTH LEAGUES CLUB

- Club received a subpoena from a member's ex-partner requesting the member's membership details and gaming information
- Club manager did not follow terms of subpoena and disclosed information directly to complainant's ex-partner instead of to the Magistrates Court.
- Privacy Commissioner declared that the Club had breached the privacy principles
- The Club was directed to:
  - **apologise in writing to the member**
  - **review its training of staff in the handling of personal information**
  - **pay the member $7500 for non-economic loss caused by the interference with her privacy.**

# AUSTRALIAN PRIVACY PRINCIPLES (OVERVIEW)

## Direct Marketing



- APP 7 – There is a general prohibition against direct marketing unless an exception applies (which relates to whether or not there is a reasonable expectation that the personal information will be used for direct marketing purposes)

## Cross border disclosure

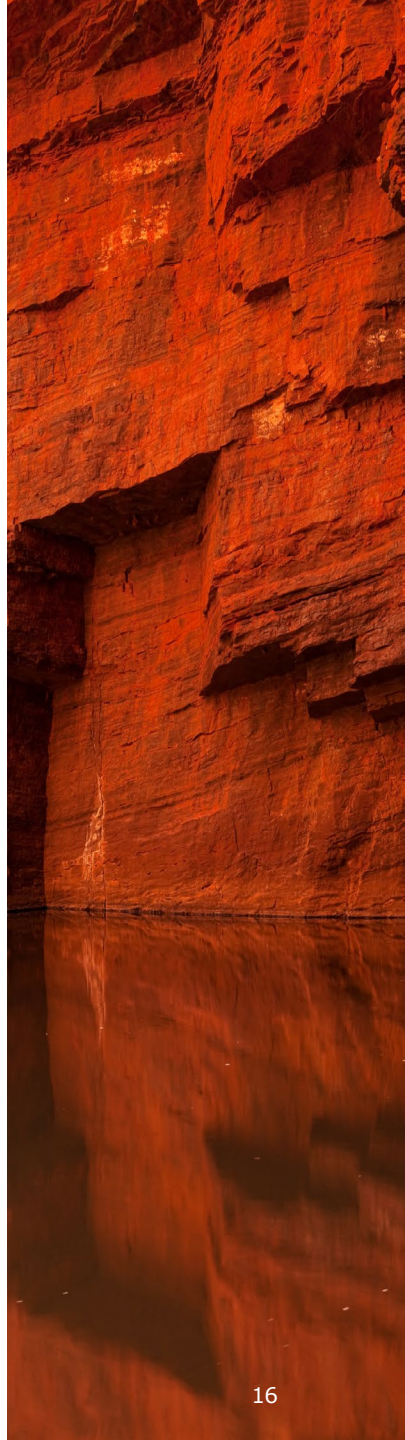
- APP 8 – Before an APP entity discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient does not breach the APPs

# Security of information

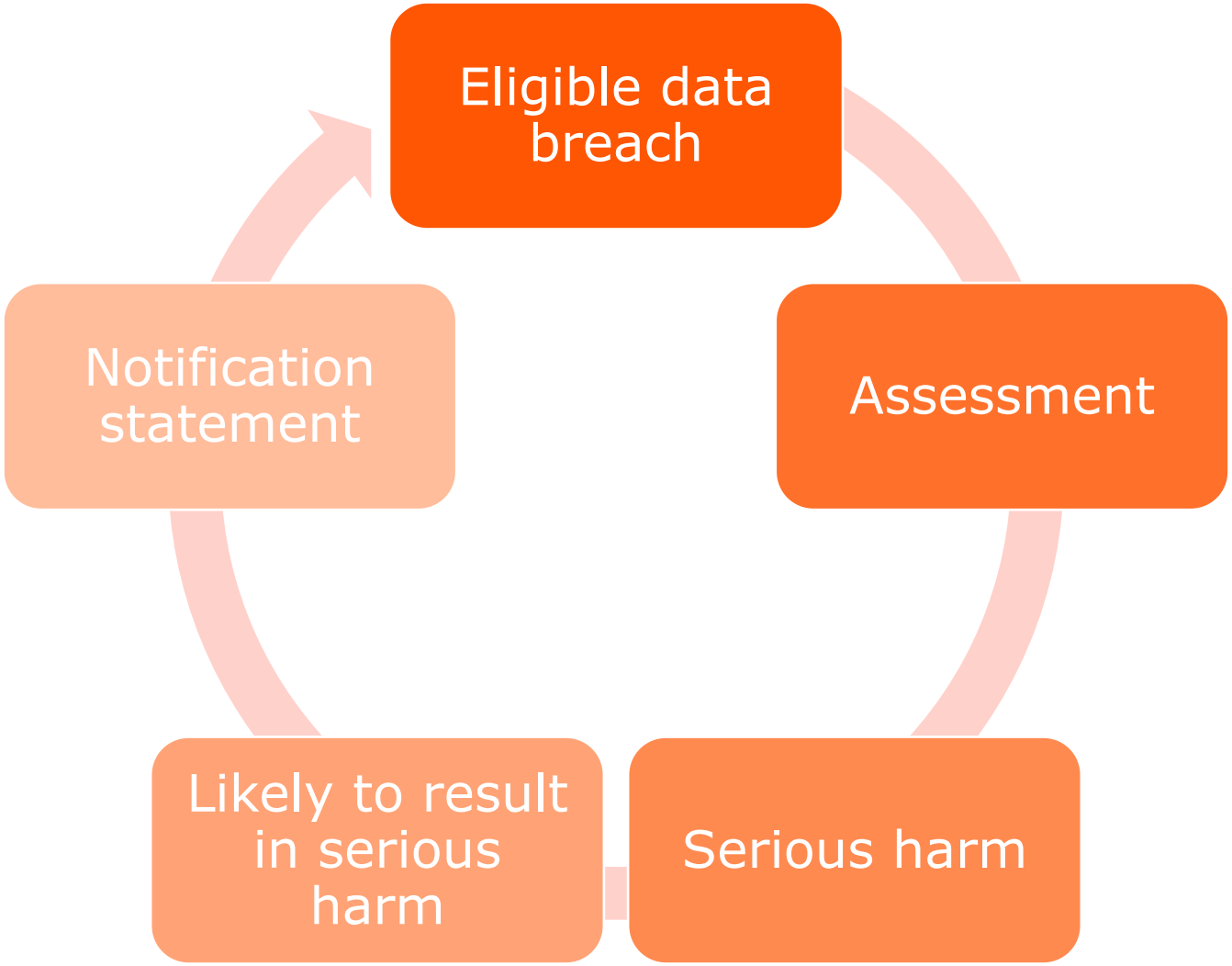
- APP 11.1 – An APP entity must take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure
- APP 11.2 – If an APP entity no longer needs the personal information for any purpose, the entity must take reasonable steps to destroy or de-identify the information

## Notification requirement

- APP entities are required to notify the Privacy Commissioner and affected individuals if there are reasonable grounds to believe that an "eligible data breach" has occurred
  - ***Timeframe:*** **As soon as reasonably practicable**
- Where an APP entity merely suspects that its data has been breached, it must undertake an assessment of the suspected "eligible data breach"
  - ***Timeframe:*** **30 days to conduct the assessment before it must report**

# KEY CONCEPTS



# ELIGIBLE DATA BREACH

- An "**eligible data breach**" happens if:
  - there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity

    **AND**

  - a reasonable person would conclude that the access, disclosure or loss is <u>likely to result in serious harm</u> to any of the individuals to whom the information relates
- Exception: Remedial Action
  - <u>Not</u> an "eligible data breach" if:
    - APP entity takes remedial action before the access, disclosure or loss results in serious harm **AND**
    - as a result of the remedial action, a reasonable person would conclude that the access, disclosure or loss would not be likely to result in serious harm

# ASSESSMENT

## If an assessment is required, it should be "reasonable and expeditious"

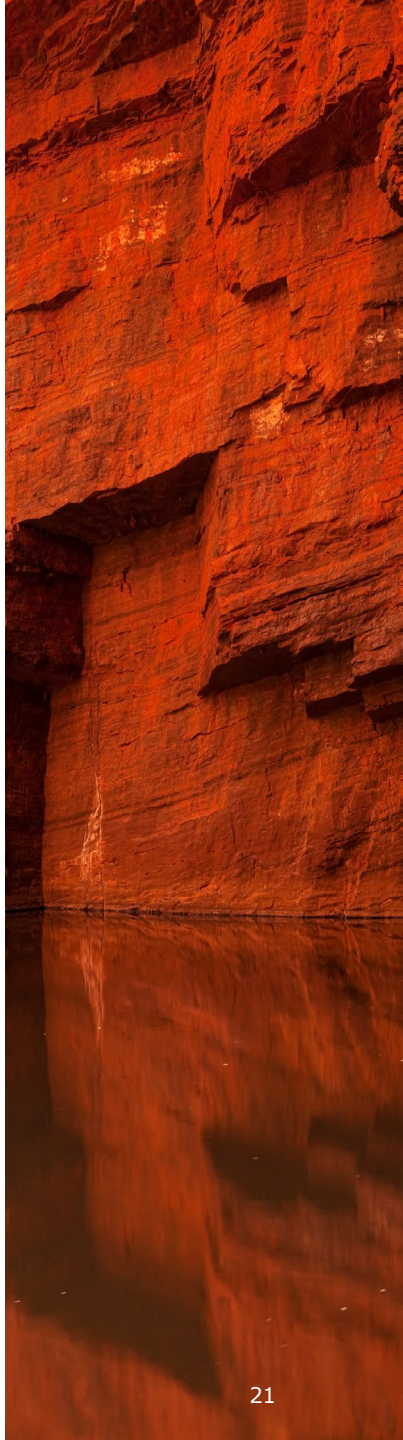
- Consider only matters which may be relevant
- Is not directly related to the size of the breach
- Conducted promptly and efficiently
- Remedial action can be attempted

# SERIOUS HARM

"**Serious harm**" could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm

# LIKELY TO RESULT IN SERIOUS HARM

- This is assessed from the perspective of a reasonable person, taking into account:
  - the kind or kinds of information
  - the sensitivity of the information
  - the nature of the harm
  - the persons, or the kinds of persons, who have obtained the information
  - if a security technology was used which was designed to make any compromised information unintelligible or meaningless to persons who are not authorised to obtain the information

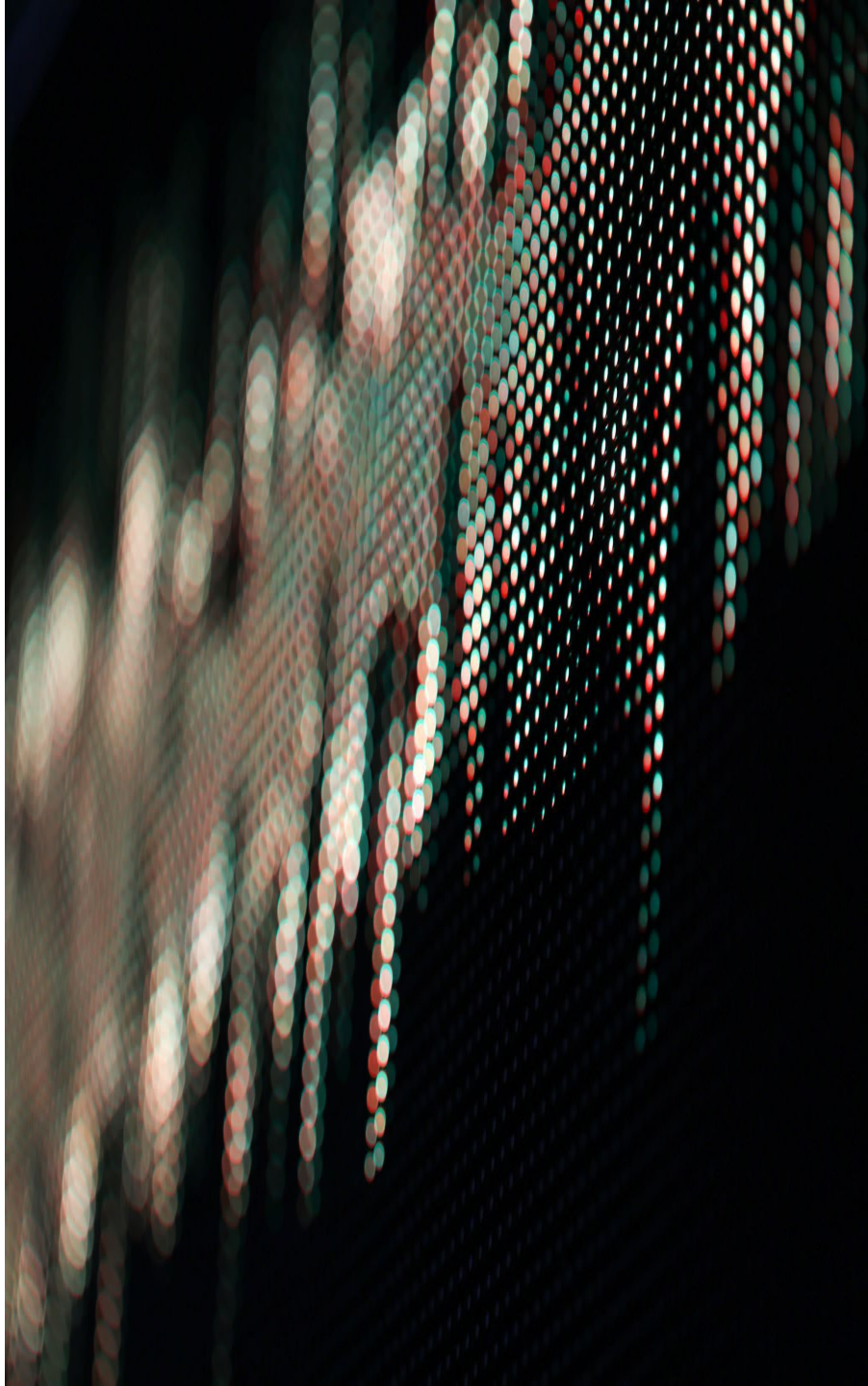


# NOTIFICATION STATEMENT

- Identity and contact details of APP entity
- Description of the eligible data breach
  - Why does the entity have reasonable grounds to believe it has happened?
- The information which has been affected
- Recommendations about steps the individual should take in response
- Method by which entity normally communicates with individual is the method to be used for data breach notification

# SERVICE PROVIDERS HANDLING INFORMATION

- If SSO has disclosed member personal information to a service provider, SSO remains responsible for the assessment and notification to any members whose information is caught in a data breach
- “Most direct” relationship with members



# OVERSEAS RECIPIENTS OF PERSONAL INFORMATION

- APP entities retain accountability for an "eligible data breach" even though that APP entity might not have responsibility for the breach due to the fact that the personal information had been disclosed to an overseas recipient (eg, cloud service provider)
- Obligations to assess breach and notify continue to apply to Australian entity

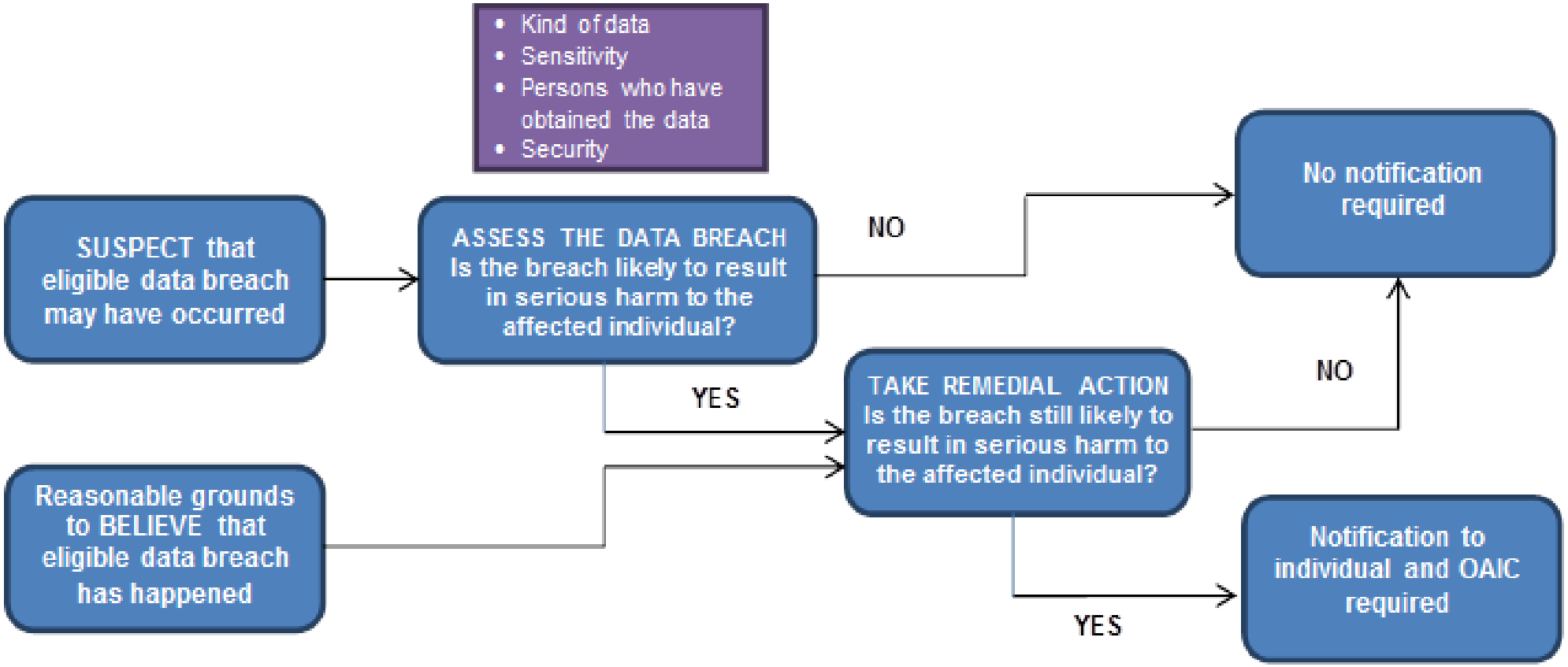
# EXAMPLE: AUSTRALIAN DEPARTMENT OF IMMIGRATION

- A staff member at the Australian Department of Immigration inadvertently sent a tour group's passport numbers, visa details and other personal information to the CEO of a company based in Hong Kong
- This email was sent in error due to the auto-complete function in Outlook
- The "tour group" was all the world leaders attending the G20 summit which included Barack Obama, Vladimir Putin and Angela Merkel.

# EXAMPLE: AUSTRALIAN DEPARTMENT OF IMMIGRATION

- **Assess the risks**
  - *What is the personal information?*
  - *Was the data encrypted?*
  - *What steps did the Government take in response?*
  - *Is the breach likely to cause serious harm to the individuals?*
- **Our view:** Unlikely to be an "eligible data breach"

# SUMMARY OF REQUIREMENTS



# CONSEQUENCES FOR NON-COMPLIANCE

## Failing to notify

- Failing to comply with any privacy laws will be taken to be an act that is an "**interference with the privacy of an individual**" and may be subject to penalties

## Privacy Commissioner's powers

- investigate complaints made by individuals
- initiate its own investigations
- accept a written undertaking
- make determinations (enforceable through court proceedings)

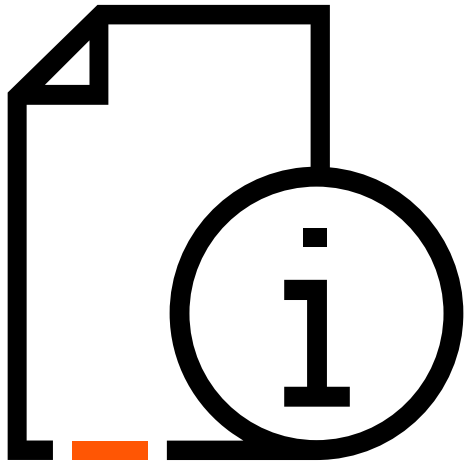
# Privacy Commissioner's powers (continued)

- Issue civil penalties for "**serious or repeated interferences of privacy**"
  - ***Current penalty:*** **up to $2.5M for individuals and up to the greater of $50M, three times value of the benefit obtained or 30% of adjusted turnover during breach period for body corporates**

## What are "serious and repeated interferences of privacy"?

# Contracts with partners

- What are the privacy implications of allowing partners access to the SSO's customer/member databases? How should the SSO structure these arrangements?
- How does this tie in with accounts in the SSO's database who have opted-out of third-party marketing?
- When the SSO provides member address details to third party mail houses, is there a requirement that we obtain a Non-Disclosure Agreement from the third party?



# Member communications

- SSO has structured its CRM privacy options so that there are certain communications that members cannot opt out of as they are essential to the administration of member accounts or are required to comply with the SSO's rules. Is this practice acceptable under privacy legislation?
- Are there any other types of communications that could/should be considered non opt-out?
- What are the rules for promotions designed to capture contact details via data cards? Can default position on the data card be "Opt-in for marketing unless opt-out box ticked"?
- The SSO has venue members and club members, can both groups receive the same communication even though signed up to different databases?

# Security of information

- What is the best practice for handling hard copy documents which contain credit card information?
- The SSO does not require customers to authenticate their identity (e.g. via stored security questions) when calling customer service to transact on their account. Does this area need to be tightened up from a privacy best practice perspective?
- Customers request to reset their passwords via social media by providing the SSO with their member number. Are there any privacy issues?

## Monitoring of website

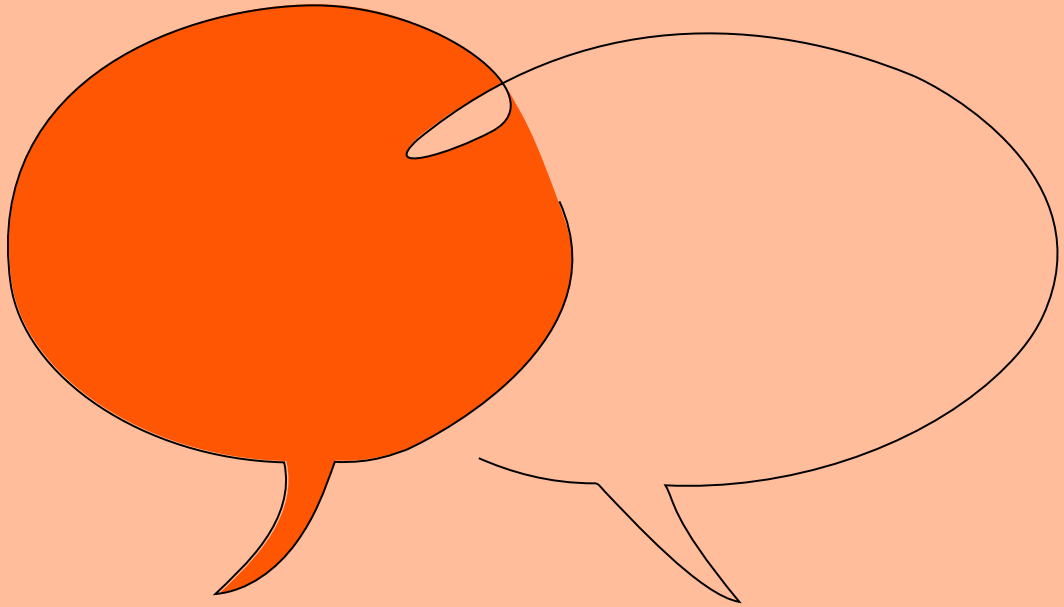
- The SSO would like to implement a tracking widget on its website called Hotjar (www.hotjar.com). This widget will allow the SSO to see how visitors are really using the website through heatmaps, recordings etc. What are the privacy implications of using such a tool?
- Are there any other legal/best practice considerations the SSO needs to be aware of?
- The SSO uses a third-party portal to provide patron access to its wi-fi network. The third party has its own privacy policy disclosed on the portal, alongside the SSO's privacy policy. Is it ok for the SSO to display multiple privacy policies?

# KEY CONTACT

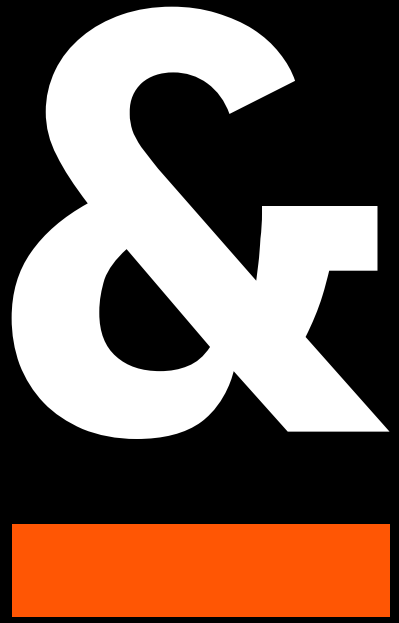
**Simon Merritt**
*Special Counsel*

**D** +61 3 9269 9579
**M** +61 413 750 025
**E** smerritt@landers.com.au

# QUESTIONS



# THANK YOU



This presentation cannot be regarded as legal advice. Although all care has been taken in preparing this presentation, readers must not alter their position or refrain from doing so in reliance on this presentation. In particular, the clauses included in this presentation are randomly selected from sample project documents and are not to be assumed to be drafting models. Where necessary, advice must be sought from competent legal practitioners. The author does not accept or undertake any duty of care relating to any part of this presentation.


**Melbourne**

**T** +61 3 9269 9000
**F** +61 3 9269 9001

**Sydney**

**T** +61 2 8020 7700
**F** +61 2 8020 7701

**Brisbane**

**T** +61 7 3456 5000
**F** +61 7 3456 5001