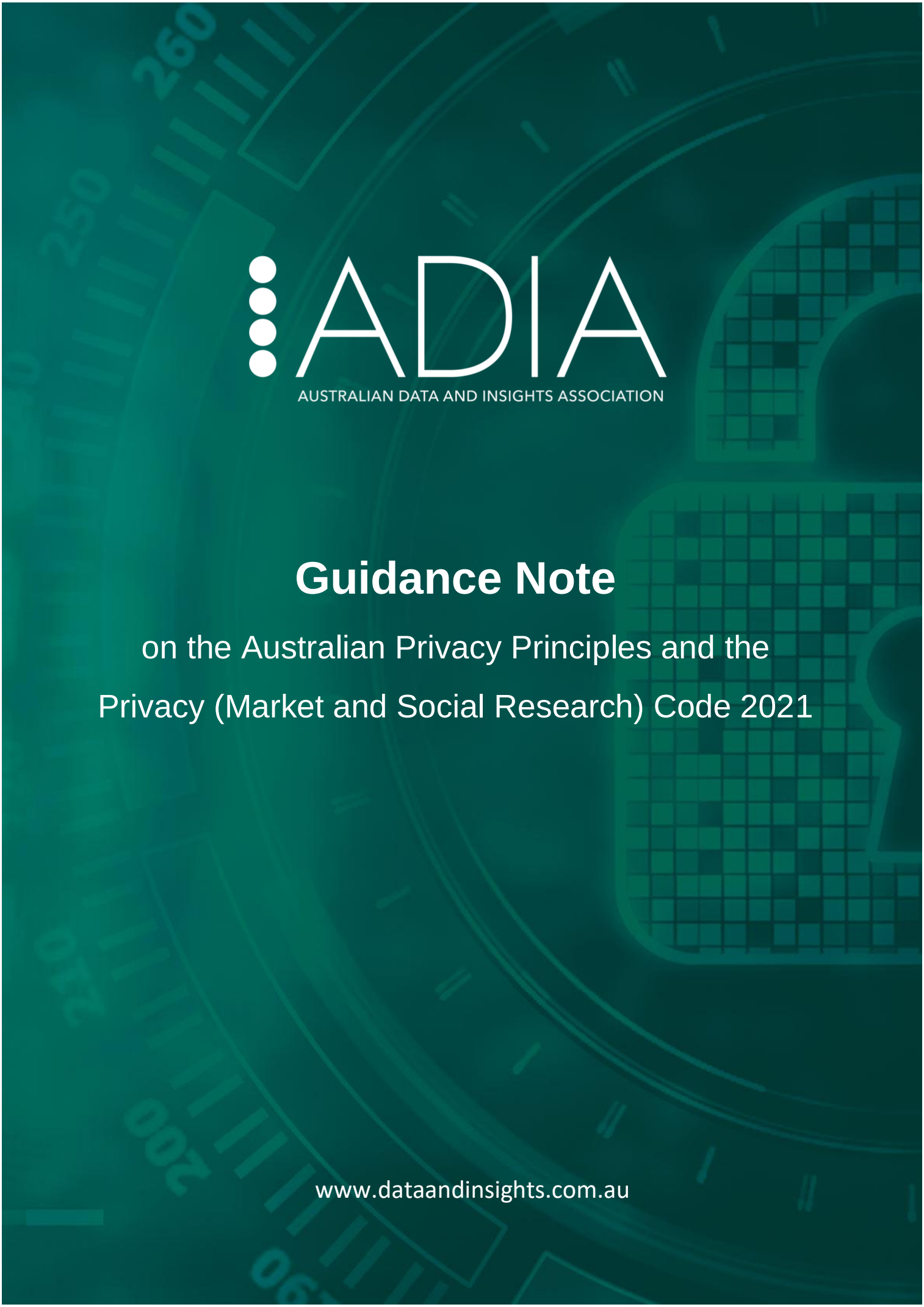


# Guidance Note

## on the Australian Privacy Principles and the Privacy (Market and Social Research) Code 2021

www.dataandinsights.com.au

# Table of Contents:

# Introduction:

Trust is critical to engagement. Now more than ever. Today's data-driven world and the number of recent high-profile data breaches have seen a growing need to ensure that personal information is always protected.

In dealing with the public and with any information entrusted to our care by them or for them, ADIA members should remember that our industry relies largely on their goodwill. When implementing the steps found in this guidance note, members should always keep the individual respondent's best interests in mind. Although the privacy act relates only to private individuals' personal information, the research, data and insights industry treats all respondents with equivalent care and respect.

This guidance note is exclusive to ADIA member organisations and is designed to complement *The Privacy Market and Social Research Code* as amended from time to time (**Privacy Code**) and support members with the implementation of data protection practices to ensure a clear understanding of the APPs and the Privacy Code.

Organisations must take reasonable steps to implement these practices, procedures and systems to ensure compliance with the Privacy Code (registered under Australian Law) and the Australian Privacy Principles.

The functions of a privacy compliance program are to:

- Establish procedures to identify and manage privacy risks;
- Ensure your organisation can respond to any privacy performance assessment or audit by the Information Commissioner; and
- Assist in defending a complaint made to the Information Commissioner.

Having a rigorous privacy compliance process in place will be imperative as consumers and regulators increase their expectations regarding appropriate data and handling. ADIA members are well placed, working under Australia's first and only registered APP Industry Privacy Code with ADIA as Administrator of the Code.

**For further information regarding the APP's and Privacy Code please contact:**

Sarah Campbell
Chief Executive Officer
ADIA
E: sarah@dataandinsights.com.au

Andrew Maher
Partner, CIE Legal
ADIA Legal Counsel
E: amaher@cielegal.com.au

## Australian Privacy Principle 1:

## Open and transparent management of personal information

### What are the obligations?

1. When handling identifiable research information, Research Organisations must take steps that are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APPs and the Code and that will enable it to deal with inquiries or complaints from individuals about its compliance with the APPs. A failure to do so may be deemed to be a breach of the Act and/or the Code which will be grounds for a complaint and/or investigation under the Act.

2. If complaints cannot be informally resolved within 30 business days, either the complainant or the research organisation may refer the complaint to ADIA. If complaints cannot be resolved to the satisfaction of the complainant or research organisation following the complaint handling process, either the complainant or the research organisation may refer the complaint to the Information Commissioner.

3. In order to meet the annual complaint reporting obligations under Part H (a) of the Code, research organisations will need to keep records during the year in a form that will allow them to report to ADIA.

4. Research organisations must also have a clearly expressed and up to date APP privacy policy that provides details about the management of personal information and identifiable information handled by the organisation.

5. In the context of identifiable research information, a privacy policy must contain the following information:

   (a) the kinds of personal information and identifiable research information that is collected and held;
   (b) how personal information and identifiable research information is collected and held;
   (c) the purposes for which personal information and identifiable research information is held, used and disclosed;
   (d) how an individual may access their personal information and identifiable research information and have it corrected;
   (e) how an individual may complain about a breach of the APPs and how the complaint will be dealt with; and
   (f) whether personal information and identifiable research information is likely to be disclosed to overseas recipients and if practicable the countries in which those recipients are located;

6. Privacy policies must be available free of charge, in an appropriate form and in the form that an individual or body requests.

### What steps should be taken to ensure compliance?

1. Update the organisation's privacy policy with the additional information required in APP 1.

2. Implement practices, procedures and systems to ensure compliance with the APPs (for further guidance on issues to consider in preparing these see **Appendix A**).

3. Implement practices, procedures and systems to deal with complaints and enquiries about compliance with the APPs (for further guidance on issues to consider in preparing these see **Appendix B**).

## Australian Privacy Principle 2:

## Anonymity and pseudonymity

### What are the obligations?

1. Research organisations must give individuals the option of not identifying themselves, or of using a pseudonym. This obligation will not apply if the organisation is required by law or through the order of a Court or Tribunal to identify themselves or it is impracticable for it to deal with the individuals who have not identified themselves or used a pseudonym.

2. Instances where it may be impracticable for a research organisation to deal with an individual anonymously or by means of a pseudonym will generally be limited to circumstances where contact details are received from a third party or where the research data (including the IP addresses in the case of online surveys) itself may potentially allow for identification.

### What steps should be taken to ensure compliance?

1. Review and assess the types of research activities where it may be impracticable to deal with individuals anonymously or using a pseudonym.

2. Where it is practicable for individuals to remain anonymous or use a pseudonym implement research practices, procedures and systems to ensure that individuals can deal with the organisation anonymously or using a pseudonym.

## Australian Privacy Principle 3:

## Collection of solicited personal information

### What are the obligations?

To comply with APP 3, research organisations must ensure the following requirements are met.

**A. Collection of Personal Information and Identifiable Research Information**

1. Research Organisations must:

   (a) not collect personal information unless the information is *reasonably necessary* for one or more of its functions or activities;
   (b) not collect identifiable research information unless the information is *reasonably necessary* for one or more research purposes;
   (c) collect personal information and identifiable research information by lawful and fair means;
   (d) only collect identifiable research information directly from an individual unless it is unreasonable or impracticable to do so; and
   (e) collect personal information about an individual from the individual unless:

      i. it has the consent of the individual to collect the information from a third party; or
      ii. it is required or authorised by law or a court/tribunal order to collect the information from a third party; or
      iii. it is impracticable to do so.

Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case. The following considerations may be relevant:

- whether the individual would reasonably expect personal information about them to be collected directly from them, or from another source;
- the sensitivity of the personal information being collected;
- whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected;
- any privacy risk if the information is collected from another source; and
- the time and cost involved of collecting directly from the individual (NB: whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances).

B. **Collection of Sensitive Information**

1. Research Organisations must not collect information about an individual that is sensitive unless the individual consents to the collection of the information and the information is reasonably

necessary for, or directly related to, one or more of its research purposes or business activities and functions, unless the collection is required or authorised by law or order of a court/tribunal.

### What steps should be taken to ensure compliance?

1. Review what information is collected to assess whether it is personal information or sensitive information.

2. In respect of personal information and sensitive information collected, assess whether it is reasonably necessary for a research purpose. If information is not reasonably necessary, it should cease to be collected.

3. In respect of sensitive information, ensure that consent is obtained from the individual at or prior to the time of collection.

4. Review collection practices, procedures and systems to ensure where it is reasonable and practicable, personal information and identifiable research information are obtained directly from individual.

5. Review collection practices, procedures and systems to ensure where personal information is obtained from a third party that consent is obtained from the individual.

## Australian Privacy Principle 4:

## Dealing with unsolicited personal information.

### What are the obligations?

1. Where unsolicited personal information is received by a research organisation, it must:

    - determine, within a reasonable period of time, whether or not it would be permitted to collect the information under APP 3 if it was solicited (the organisation may use or disclose the information for the purpose of making any such determination); and
    - if it would not be permitted to collect the information, it must destroy the information or ensure it is de-identified as soon as practicable; otherwise
    - it can retain the information in accordance with APPs 5 to 13.

2. Under APP 4, unsolicited information is afforded the same protections as solicited information.

### What steps should be taken to ensure compliance?

1. Review whether unsolicited personal information received or is likely to be received.

2. Review current practices, procedures and systems for dealing with unsolicited information to ensure a system is in place to:
    - make a determination regarding whether the collection of the unsolicited information would be permitted; and
    - destroy or de-identify the information as required; or

- ensure the information is retained in accordance with APPs 5 – 13.

## Australian Privacy Principle 5:

## Notification of the collection of personal information

### What are the obligations?

**A. Collection of Personal Information**

1. An organisation must provide to an individual either before or at the time of collecting any personal information (in the form of a privacy collection statement) the following:

    - its identity as the organisation collecting the information and contact details;
    - the purpose for which the information is collected;
    - the organisations to which information is usually disclosed;
    - any law or court/tribunal that requires the information to be collected;
    - the fact they can access their information;
    - the main consequences, if any, of not providing the information; and
    - that the privacy policy explains:
        - how an individual may access and correct personal information held about them; and
        - how they may complain about an APP breach and how the complaint will be dealt with; and
        - whether personal information is likely to be disclosed to overseas recipients and if so (and practicable) the countries in which those recipients are located.

2. If personal information is collected from someone other than the individual, reasonable steps must be made to notify the individual that they have collected the information and the circumstances of the collection.

**B. Collecting identifiable research information**

1. A research organisation must provide to an individual (in the form of a privacy collection statement) at or before the time of collection of identifiable research information:

    (a) its identity as the research organisation collecting the information;
    (b) the position title, telephone number and email address of a contact in the research organisation who handles its privacy related enquires and complaints details;
    (c) if the research organisation has collected personal information from a third party (such as a client or list provider), the source of the research sample and the circumstances of the collection the fact they may withdraw their consent;
    (d) any law or court/tribunal that requires the information to be collected;
    (e) that the information will be used only for market and social media purposes and that no other use will be made of the information (subject to any exemptions that apply);

(f) the fact that research data collected is routinely de-identified (if this applies) and how long research information is likely to remain identifiable;
(g) the organisations to which information is usually disclosed;
(h) that if the individual participates in the research, there is a reasonable likelihood that they will be re-contacted for market and social research purposes except where the research organisation has genuine research concerns;
(i) the fact that the research organisation wishes to disclose identifiable research information to a client organisation (if this applies) and if so **obtain their consent** to do so;
(j) the fact the individual can access their identifiable research information prior to it being de-identified or destroyed;
(k) if applicable, that individual may request to have their identifiable research information de-identified or destroyed; and
(l) that the research privacy policy explains:

i. How an individual may access and correct personal information held about them; and
ii. How they may complain about an APP breach and how the complaint will be dealt with; and
iii. Whether personal information is likely to be disclosed to overseas recipients and if so (and practicable) the countries in which those recipients are located.

2. If a research organisation collects personal or research information from a third party (such as another householder or member of the family), it should take reasonable steps to ensure that individual is made aware of the matters listed above.
3. If the research organisation has collected personal information from a third party (such as a client or list provider), it must disclose the source of this information no later than at the end of the collection of the research information unless there are genuine research concerns or a compelling reason not to do so. It must also ensure that at least one of the following applies:

(a) The information was originally collected is related to the research being conducted and the individual would reasonably expect to be contacted or invited to participate in the research;
(b) Individuals have consented to their information being disclosed to the research organisation for research purposes; or
(c) A readily accessible means exists to withdraw consent to being included on the list (and this has been stated to the individual at or before the time of collection.

***Further explanatory information is available in the Privacy (Market and Social Research) Code 2021.***

## What steps should be taken to ensure compliance?

1. Review all collection statements for collecting personal information and identifiable research information and update to comply with APP 5 and the Code requirements. A template market and social research collection statement is enclosed behind **Appendix C.**

2. Review collection practices, procedures and systems to ensure where personal information is obtained from a third party that consents have been obtained from the individual.

3. Where personal information may be obtained from a third party, develop a process and procedures to ensure individuals are notified about third party collection in accordance with the APPs and the Code.

## Australian Privacy Principle 6:

## Use or disclosure of personal information

### What are the obligations?

**A. Personal Information (i.e., not research data)**

1. Personal information can only be used or disclosed for the primary purpose of its collection unless (exceptions do not apply to use for direct marketing or government related identifiers):

- the individual has consented to the use or disclosure of the information;
- for personal information, the purpose for disclosure is directly related to the primary purpose (**secondary purpose**) and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
- for sensitive information, the purpose for disclosure is directly related to the primary purpose (**secondary purpose**);
- the use or disclosure is required by law or court/tribunal order;
- the disclosure is required to lessen or prevent serious threat to life, health or safety of an individual or if it is impracticable to obtain the individuals consent, if it is required to locate a missing person or necessary to report illegal or unlawful behaviour; or
- the disclosure is made to a related body corporate.

**B. Identifiable research information**

1. Research organisations must not use or disclose identifiable research information for any purpose other than the primary research purpose, or directly related secondary research purpose except with the consent of the individual or if it is required by law.

2. Where a research discloses identifiable research information for a research purpose, it must ensure:
   (a) Only that part of the information considered necessary for the research purpose is disclosed;
   (b) If the research could be achieved using de-identified data, it is de-identified prior to disclosure; and
   (c) Where the recipient is the client, the consent of the individuals has been obtained (except where the personal information being disclosed to the client concerns individuals' research status and this cannot be linked to any research data and the research organisation has obtained the agreement of the client regarding restricting the use of the

individuals' research status for the purpose of regulating frequency of contact with the individual).

### What steps should be taken to ensure compliance?

1. Review for what purposes the organisation uses and discloses personal information.
2. Where disclosure or use may vary from the primary purpose, ensure steps are implemented to obtain the individual's consent; and
3. Ensure practices, procedures and systems for the use and disclosure of personal and sensitive information are implemented.

*For additional information please see the Office of the Australian Information Commissioner (OAIC) Privacy Management Plan template.*

## Australian Privacy Principle 7:

## Direct marketing

### What are the obligations?

1. Research organisations are not permitted to use or disclose identifiable research information about an individual for the purpose of direct marketing.

2. In respect of other personal information held by the organisation, it must not use or disclose that information for the purpose of direct marketing unless:

   - the information is collected directly from the individual and the individual reasonably expects direct marketing and so long as there is a simple means to opt out and the individual has not opted out; or
   - the information is collected from a third party or the individual does not reasonably expect direct marketing and the organisation has obtained consent (or it is impracticable to do so) **and** it includes a prominent statement in the direct marketing telling the individual that they may opt out **and** the individual has not opted out.

3. Direct marketing with sensitive information is only permitted with express consent.

4. Where an individual has been sent direct marketing and he/she:
   (a) opts out;
   (b) request that personal information not be disclosed to facilitate direct marketing by another; or
   (c) request the organisation provide the source of the personal information,

   then it must give effect to the request within a reasonable period of time.

### What steps should be taken to ensure compliance?

1. Review policies and practices to ensure they are adequate to protect identifiable research information from being used for direct marketing.

2. Review any other direct marketing activities to assess whether they use or disclose personal information (including to third party providers).

3. Where personal information is used and disclosed for direct marketing determine whether this is something the individual would reasonably expect. If not, the use of personal information for direct marketing must stop before the APPs are implemented.

4. If an organisation wants to use personal information for direct marketing, it must ensure processes, procedures and systems are in place to:

   (a) obtain individuals' consent;
   (b) ensure it can meet requests to opt out; and
   (c) provide the source of the personal information used for the direct marketing.

## Australian Privacy Principle 8:

## Cross-border disclosure of personal information

### What are the obligations?

1. Before disclosing any personal information and identifiable research information to an overseas recipient, research organisations must take reasonable steps to ensure the overseas recipient does not breach the APPs.
2. Where there are overseas disclosures of identifiable research information, that information remains governed by the APPs and the Privacy Act but may also become subject to data protection laws of other jurisdictions, including the General Data Protection Regulation of the European Union.
3. Research organisations will, in certain circumstances, be responsible for a breach committed by the overseas recipient unless it:

   (a) reasonably believes the overseas recipient to be subject to a law or binding scheme that is substantially similar to the APPs **and** there are mechanisms in place which allow the individual to enforce the protection of that law or binding scheme; or
   (b) the individual has consented to the disclosure, after having been expressly informed that APP 8.1 will not apply to the disclosure if consent is provided; or
   (c) disclosure is required by court order; or
   (d) it is required for a permitted health or safety reason.

### What steps should be taken to ensure compliance?

1. Review all disclosures of personal information to overseas locations and identify those countries where personal information may be sent (Note: remember to update the privacy policy with this information).
2. Conduct a review of the privacy laws (i.e., GDPR) if any in the countries where personal information is currently sent.
3. Review contracts (such as outsourcing agreements) that are in place to assess whether they can be relied upon to enforce the APPs on the overseas recipient. Where contractual mechanisms

are not sufficient to enforce the APPs, organisations should seek to have the contracts amended or identify new providers that can ensure compliance with APP 8.

Review practices, procedures and systems for sending personal information overseas including how individuals' consent will be obtained.

*Note: Member organisations are also encouraged to review State and Territory privacy laws.*

## Australian Privacy Principle 9:

## Adoption use or disclosure of Government related identifiers

### What are the obligations?

1. Organisations must not adopt, use or disclose a government related identifier (including those of State and Territory authorities) of an individual as its own identifier unless the use or disclosure:
    - is reasonably necessary for the organisation to verify the individual for the purpose of the organisation's activities or functions;
    - is reasonably necessary for the organisation to fulfil its obligations to a government agency or a State or Territory authority;
    - is required by a law or court or tribunal order; or
    - is a permitted health or safety situation or a law enforcement related activity.

### What steps should be taken to ensure compliance?

1. Review whether your organisation collects government related identifiers.
2. If it does collect government related identifiers, is it permitted to use or disclose those identifiers under the exceptions?
3. Review practices, procedures and systems for the collection, use or disclosure of government related identifiers.

## Australian Privacy Principle 10:

## Quality of personal information

### What are the obligations?

1. Research organisations must:
    - In respect of personal information collected (such as contact details and research status):
        - take steps that are reasonable in the circumstances to ensure that the information is accurate, up to date and complete;
        - take steps that are reasonable in the circumstances to ensure that any use or disclosure of the information is accurate, up to date, complete and relevant (having regard to the purpose of the use or disclosure); and
    - In respect of identifiable research information:
        - ensure that responses are accurately recorded and complete at the time of collection;

- warrant that the information is accurate and complete at the time of collection and ensure the disclosure is relevant (having regard to the purpose of the use or disclosure and the research being conducted)

### What steps should be taken to ensure compliance?

1. Review what steps are currently taken to ensure personal information such as research status and contact details are up to date, complete and accurate and in respect of disclosure, that it is relevant.
2. Review what steps are currently taken to ensure identifiable research information is complete and accurate at the time of collection and its disclosure relevant.
3. Implement practices, procedures and systems to ensure personal information collected is kept up to date, is accurate and complete and identifiable research information is accurate and complete at the time of collection.

## Australian Privacy Principle 11:

## Security of personal information

### What are the obligations?

1. If an organisation holds personal information, it must take reasonable steps to protect the information from misuse, interference, loss, unauthorised access, modification or disclosure. The inclusion of the requirement to protect information from "interference" is intended to recognise that attacks on personal information may not be limited to misuse or loss but may interfere with information. This element may require research organisations to put in place additional measures, which are reasonable in the circumstances, to protect against computer attacks and other interferences.

2. Research organisations must take reasonable steps to destroy or de-identify personal information in the following circumstance:
   - information is held about an individual; and
   - it is no long longer reasonably needed for any purpose directly or indirectly related to a business activity; and
   - the information is not contained in a Commonwealth record; and
   - it is not required to be retained under an Australian, law, court or tribunal.

3. Research organisations must also comply with the following additional obligations to destroy or de-identify identifiable research information:

    a. To destroy or de-identify identifiable research information once it is no longer necessary for research purposes;
    b. If a research organisation wishes to de-identify information that exists in hard copy form, the information must be moved to another medium, de-identified and the physical records destroyed;
    c. Where it is necessary to retain identifiable research information, identifiable details (such as contact details) must if practicable be stored separately from other information with measures in place (such as encryption) to ensure the identity of individuals cannot be revealed; and
    d. Take reasonable steps to ensure that any identifiable research information it discloses:
        i. will be used in accordance with the Code;
        ii. will be protected by the recipient from misuse, interference, loss, unauthorised access, modification or disclosure; and
        iii. will only be disclosed by the recipient for a specified limited purpose and will be destroyed or de-identified once the purpose has been achieved.

## What steps should be taken to ensure compliance?

1. Review what steps are currently taken to ensure personal information and identifiable research information collected is protected from misuse, interference, loss and from unauthorised access, modification or disclosure.
2. Appropriate security safeguards and measures for protecting personal information and identifiable research information are in place including strategies to ensure:

    (a) Governance arrangements to implement and maintain information security plans and measures;
    (b) Effective ICT security to protect computer hardware and data such as encryption, authentication requirements, software security network security and back-ups;
    (c) Response plans in the event of a data breach;
    (d) Physical security to control access to the organisations worksite;
    (e) Personnel security and privacy training;
    (f) Workplace policies regarding privacy; and
    (g) Regular review and monitoring of privacy requirements.

3. Review current processes are in place to destroy or de-identify data when it is no longer required for an authorised purpose.
4. If an organisation wishes to de-identify information received in physical form, ensure processes are in place to transfer to the information to a new medium and have the physical copy destroyed.
5. Implement practices, procedures and systems to ensure personal information is destroyed or de-identified when it is no longer required.

6. Implement processes and systems to ensure any identifiable research information that is retained is held separately from identifying information such as individuals' contact details.

*See further OAIC, Guideline to securing personal information, June 2018 available here. Also, OAIC. Data breach preparation and response: A guide to managing data breaches with the Privacy Act.*

## Australian Privacy Principle 12:

## Access to personal information

### What are the obligations?

1. If a research organisation holds personal information or identifiable research information about an individual, it is required to (on request) give the individual access to that information, unless certain exceptions apply. Organisations are required to respond to all requests within a reasonable period of time, as well as give access to the information in the manner requested by the individual.

2. Exemptions include:
    - Risks to life, health or safety;
    - An unreasonable impact on the privacy of others;
    - Frivolous or vexatious requests (such as repeat requests or requests that have already been provided, requests that contain offensive or abusive language);
    - Information relating to legal proceedings, and would not be accessible in discovery;
    - Information which would prejudice negotiations with the individual;
    - Where giving access would be unlawful; and
    - Situations where there is reason to suspect that an unlawful activity or serious misconduct has occurred and giving access would likely prejudice the taking of appropriate action.

3. If organisations refuse access, they are required to inform the applicant of the reasons for the refusal and the mechanisms available to complain about the refusal. Should access be granted, organisations are entitled to charge reasonable access charges.

### What steps should be taken to ensure compliance?

1. Review the means by which your organisation currently responds to requests from individuals for access to personal information and identifiable research information.

2. Implement processes, procedures and systems for responding to individuals' requests to access personal information or identifiable research information including timeframes for responding, the manner in which access is given, the provision of written reasons and charges for access (see **Appendix B** for further guidance).

# Australian Privacy Principle 13:

# Correction of personal information

## What are the obligations?

**Correction**

If an organisation holds personal information or identifiable research information (such as contact details or research status) other than research data about an individual and it is satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading or the individual requests your organisation to correct information, it must take reasonable steps to correct information, and ensure it is accurate, up to date, complete and not misleading.

Where a research organisation receives a request to correct research data, it should:

(a) Explain it may not be possible to correct research data where it must remain an accurate and complete record of the information at the time of collection; and
(b) If requested, associate a statement with the information that the individual believes the information is inaccurate, out of date, incomplete, irrelevant or misleading.

**Requests for the destruction or de-identification of research information**

Research organisations must accept and act on requests for identifiable research information to be destroyed or de-identified, except in the following circumstances:

(a) The request is frivolous or vexations (e.g. it is trivial, is being made to pursue some other grievance against the organisation, is a repeated request or is made principally to create inconvenience);
(b) Destruction or de-identification would have an unreasonable impact on the privacy of other individuals;
(c) The research organisation is contractually obliged to retain the information; and
(d) Destruction or de-identification would;
    a. Pose a health or safety risk;
    b. Prejudice negotiations with the individual;
    c. Be unlawful;
    d. It is required to be retained by a law or court/tribunal order;
    e. Prejudice a law enforcement related activity.

N**otification**

If an organisation corrects personal information about an individual that it previously disclosed to another APP entity, and the individual requests the organisation to notify the other APP entity of the correction, the organisation must take reasonable steps to give that notification unless it is impracticable or unlawful to do so.

**Refusal**

If an organisation refuses to correct the personal information as requested by the individual, it must give the individual written notice that sets out the reasons for refusal to the extent that it would be unreasonable to do so, the mechanisms available to complain about the refusal and any other matter prescribed by regulations.

**Request to associate a statement**

If an organisation refuses to correct the personal information requested by the individual and the individual requests it to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading, then the organisation must take reasonable steps to associate the statement in a way to make it apparent to the users of information.

**Dealing with requests**

If a request is made of correction or associate a statement, the organisation must respond to the request within a reasonable period after request is made and must not charge the individual for making the request, correcting the personal information or for associating the statement with the personal information.

## What steps should be taken to ensure compliance?

1. Review the means by which your organisation currently responds to requests from individuals for correction to personal information.
2. Implement processes, procedures and systems for responding to individuals' requests to correct personal information including timeframes for responding, the provision of written reasons and third-party notification (see **Appendix B** for further guidance).

<end>

# Overview: Notifiable Data Breaches scheme

**What is the Notifiable Data Breaches (NDB) scheme?**

The Notifiable Data Breaches (NDB) scheme requires organisations covered by the Australian *Privacy Act 1988* (Privacy Act) to notify any individuals likely to be at risk of serious harm by a data breach.

**Who must comply with the NDB scheme?**

The NDB scheme applies to businesses (with an annual turnover of $3 million or more), Australian Government agencies, and other organisations that are already required by the Privacy Act to keep information secure.

**What is a Notifiable Data Breach?**

- A Notifiable Data Breach is a data breach that is likely to result in '**serious harm'** to any of the individuals to whom the information relates.
- A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

Examples of a data breach may include when:

- A device containing customers' personal information is lost or stolen;
- A database containing personal information is hacked;
- Personal information is mistakenly provided to the wrong person.

**Which data breaches are notifiable?**

Not all data breaches are notifiable.

The NDB scheme only requires organisations to notify when there is a data breach that is likely to result in **serious harm** to any individual to whom the information relates.

Under the *Office of the Australian Information Commissioner* (OAIC) guidelines, an eligible data breach occurs when three criteria are met:

1. There is unauthorised access to, or unauthorised disclosure of personal information, or loss of personal information, that an entity holds;
2. This is likely to result in serious harm to one or more individuals, and
3. The entity has not been able to prevent the likely risk of serious harm with remedial action.

- **'Serious harm'** can be psychological, emotional, physical, reputational, or other forms of harm.
- Understanding whether serious harm is likely or not requires an evaluation of the context of the breach.

Exceptions to the NDB scheme will apply for some data breaches, meaning that notification to individuals or to the Commissioner may not be required.

For further information - https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/entities-covered-by-the-ndb-scheme.

**Assessing suspected data breaches**

Organisations that suspect a data breach may have occurred are required to undertake a quick assessment to determine if the data breach is likely to result in **serious harm**.

For research organisations (suppliers) it is important that everyone involved in handling or control of data should consider they may have a part to play in resolving a response and remedy as soon as possible after a breach, for the benefit of the data subject for whom the clock may be ticking.

It may be possible to avoid transference of liability while at the same time creating an obligation for everyone involved to cooperate, assist or contribute any necessary information to a joint quick response effort.

**Can I take remedial action?**

Yes, it is recommended that you do so as soon as practicable.

- If you take remedial action that prevents the likelihood of **serious harm** occurring, then the breach is not an eligible data breach.
- For breaches where personal information is lost, the remedial cation is adequate if it prevents the unauthorised access or disclosure of personal information.

**Appropriate remedial action should:**

- Be undertaken as quickly as possible (so the individuals affected have maximum chance to respond urgently enough to mitigate their own risk),
- be simply and clearly expressed (so it can be easily understood by non-experts),
- focus on helping the data subject identify what, if anything, they may need or wish to do themselves as mitigation or remedy,
- be frank and concrete enough so that the potentially data subjects can get a good picture of what has actually happened (so they can draw their own conclusions about if and how this might affect them).

**Notification of an eligible data breach**

Notification of a data breach supports good privacy practice.

Where an organisation becomes aware that there are reasonable grounds to believe an eligible data breach has occurred, they are obligated to notify individuals at risk of serious harm and the OAIC as soon as practicable.

This notification must set out:

- the identity and contact details of the organisation;
- a description of the data breach;
- the kinds of information concerned and;
- recommendations about the steps individuals should take in response to the data breach.

*ADIA, as the Code Administrator, has issued instructions for the reporting of complaints, including the method of reporting, which is likely to involve a simple completion of an on-line form.*

- Research Organisations must notify eligible data breaches to the Australian Information Commissioner and otherwise comply with the eligible data breach requirements of the Privacy Act.
- Research Organisations should also inform the Code Administrator (ADIA) of any notification of an eligible data breach as provided to the Australian Information Commissioner and of any reasonably likely or actual serious data breach (whether or not a notifiable eligible data breach) that demonstrates a significant vulnerability of other Research Organisations in handling of identifiable research information that might reasonably be expected to be mitigated by appropriate action taken by Research Organisations generally.
- Research Organisations must report annually, by 31 August, to ADIA (the Code Administrator) on the number, nature and outcomes of any complaints received about Breaches of this Code.

# General Data Protection Regulation (GDPR)

**What is GDPR?**

The **European Union's General Data Protection Regulation** 2016/679 (the GDPR) contains data protection requirements that extend the scope of the EU data protection law to all foreign companies processing personal data of EU residents (i.e. All EU countries and the UK are required to work under the new data laws).

**When did it commence?**

The GDPR commenced on the 25 May 2018. Any business found in breach of the law will be liable for fines of up to 4% of worldwide annual turnover.

**Who is affected?**

The GDPR applies to all businesses that process data and operate within the EU. It also applies to any business that monitor EU residents or offer goods or services to EU residents.

**What does it mean for Australian Research companies?**

Australian businesses of any size may need to comply if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.

**For ADIA member companies the GDPR and the Australian Privacy Act 1988 (or the Privacy Code) share many common requirements, including to:**

- implement a *privacy by design* approach to compliance;
- be able to demonstrate compliance with privacy principles and obligations;
- adopt transparent information handling practices.

There are also some notable differences, including certain rights of individuals, such as:

- the right to be forgotten (GDPR gives individuals the right to erasure),
- stronger consent provisions (the GDPR states that consent must be freely given, specific, informed and an unambiguous indication of the data subjects wishes),
- the right for citizens to access and correct their personal data once collected by marketing or other bodies (GDPR).

Australian businesses should determine whether they need to comply with the GDPR and if so, take steps to ensure their personal data handling practices comply with the GDPR before commencement.

**Australian businesses that may be covered by the GDPR include:**

- an Australian business with an office in the EU.
- an Australian business whose website targets EU customers for example by enabling them to order goods or services in a European language (other than English) or enabling payment in euros.
- an Australian business whose website mentions customers or users in the EU.
- an Australian business that tracks individuals in the EU on the internet and uses data processing techniques to profile individuals to analyse and predict personal preferences, behaviours and attitudes.

**What does it mean for conducting research in the EU?**

Under the GDPR, all researchers, whether employed within an agency, working independently or based within a client's research department, need to ensure that they understand the legal basis being used for collecting, using, storing, sharing or otherwise processing personal data at all stages, as part of their research project.

For further information, OAIC Privacy guidance and advice

# APPENDIX A

Organisations are required to take reasonable steps to implement practices, procedures and systems to ensure it will comply with the APPs and the Privacy Code. The functions of a compliance program are to:

- Establish procedures to identify and manage privacy risks;
- Ensure your organisation is able to respond to any privacy performance assessment or audit by the Information Commissioner; and
- Assist in defending a complaint made to the Information Commissioner.

The following information provides some guidance on the issues organisations should consider in developing a robust and data privacy compliance program.

ADIA has also developed a suite of training modules available here.

**1. Privacy Officer**

Organisations should appoint a staff member to act as its privacy officer. The privacy officer should implement and oversee a privacy compliance strategy and respond to privacy enquiries and complaints. The privacy officer should also have authority to:

- undertake a privacy review of existing systems to assess how your organisation collects, uses, stores and discloses personal and/or sensitive information
- establish systems to ensure compliance with the APPs
- maintain and review logs of enquiries and complaints log to identify and remedy any common enquiries or systemic complaints
- provide regular reports to management identifying any privacy risks.

**2. Training about the APPs and the Code**

Organisations should ensure its staff are familiar with the APPs and the Code and are aware of how they impact on its business practices. Training on the privacy laws and the privacy policy should be provided to all staff within the organisation. *For further information please contact ADIA.*

**3. Conducting a privacy review**

The purpose of a privacy review is to analyse an organisations' personal information flows, including:

- What personal and/or sensitive information has been collected and from whom?
- How is personal information collected?
- For what purpose is the information collected and does it properly relate to one or more business functions or activities?
- How will the information be used?
- How will the information be stored and disposed?

- How can an individual access their personal information?
- What information is disclosed to third parties?
- What consents are in place for use or disclosure?
- How is the information maintained so that it is up to date, accurate and relevant?
- How are complaints and enquiries handled?
- Is personal information sent overseas and if so where?

**4. Update and maintain privacy policy and collection statements.**

Update the privacy policy and collection statement(s) to comply with the APPs and to align with the manner in which it uses and discloses personal information. Audits should be conducted at regular intervals to identify and respond to any privacy compliance risks.

**5. Conduct Privacy Risk Assessments (PIA) for new projects.**

A PIA is process should be adopted to understand personal information flows and privacy impacts in respect of any new project to be undertaken. This will help to manage privacy risks during the course of a project and avoid breaches of the APPs.

In respect of any project to be undertaken, a threshold assessment should be conducted to assess whether your organisation will be collecting, using or disclosing any personal information. If the answer to this question is 'yes', your organisation should undertake a PIA to identify and assess possible privacy issues.

A PIA should identify how personal information will be collected, used and disclosed and how this accords with the APPs and the privacy policy.

Further information in respect of the process for conducting a PIA, including a guidance note and checklist, can be obtained from the following OAIC website - https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

**6. Privacy procedures and security**

Organisations should prepare policies and guidelines in respect of:

- The collection, management and use of contact lists;
- Provisions to deal with privacy in respect of any outsourcing or supplier contracts where personal information may be handled;
- Data security practices and procedures (including encryption, firewalls, restricted access and regular password changes, anti-virus software and backups to be stored securely in a separate location); and
- The removal, destruction or de-identification of data that is no longer required;

# APPENDIX B

Organisations should have practices, procedures and systems in place for handling enquiries and complaints with respect to its compliance with the APPs and the Privacy Code. To ensure the process is fair and consistent, complaints and enquiries should be referred to a single point of contact being the Privacy Officer. Details of complaints should also be logged to make sure that any systemic issues are identified and acted upon.

**Below is a recommended process for dealing with privacy breaches, complaints and enquiries about personal information held by an organisation.**

| | **Procedure** | **Timeline** |
|---|---|---|
| 1 | Notify key internal personnel (e.g., privacy officer, General Manager, Managing Director) of the suspected data breach. | Recommend ASAP. No longer than 7 days. |
| 2. | Contain the suspected (or known) breach where possible. | ASAP |
| 3. | Take remedial action where possible (e.g., take steps to recover lost information before unauthorised access occurs). | ASAP |
| 4. | Assess whether the data breach is likely to result in **serious harm**.<br>a. Initiate – Investigate – Evaluate<br>If the Privacy Officer determines there has been a breach of the APPs he/she will, upon notification to the complainant, advise the relevant personnel in writing of any action required to remedy the breach. | ASAP.<br>Maximum 30 days from date of receipt. |
| 5. | If serious harm is likely:<br>**a.** Notify individual/s at risk of serious harm<br>**b.** Inform ADIA (ADIA@ADIA.com.au)<br>**c.** Notify the Australian Information Commissioner (https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB<br>Timeline: If NDB notify respondent/s ASAP. | If NDB notify respondent/s ASAP. |
| 6. | Implement prevention mechanism to ensure the breach is not repeated. | |

**Recommended Inquiry, access and correction handling procedure below.**

| | Procedure | Timeline |
|---|---|---|
| 1. | An inquiry relating to privacy is received. | Recommend ASAP. No longer than 7 days. |
| 2. | Inquiry must be forwarded to the Privacy Officer. | Recommend ASAP. No longer than 7 days. |
| 3. | The Privacy Officer must respond in writing to the enquiry. | Within 30 days. |
| 4(a) | If the inquiry included a request for personal information or identifiable research information, Privacy Officer must determine whether access to the information will be provided. | 14 days from receipt of request |
| 4(b) | If the individual is to be given access to the information, Privacy Officer to provide individual access to the information in the form requested. | 30 days from determination |
| 4(c) | If access to the information is refused, Privacy Officer must inform the individual in writing of the reasons for refusal and inform him/her of complaint process. | 30 days from determination |
| 5(a) | If the enquiry included a request to correct or destroy or de-identify personal information, Privacy Officer must determine whether to update the information. | 14 days from receipt of request |
| 5(b) | If the information is to be corrected, de-identified or destroyed, Privacy Officer to notify relevant personnel to have the information updated. | Upon determination |
| 5(c) | If the update to information is refused, Privacy Officer must inform the individual in writing of the reasons for refusal and inform them of complaint process. | 30 days from determination |
| 5(d) | Privacy Officer to confirm information has been corrected, destroyed or de-identified | 30 days from notification |
| 5(e) | Privacy Officer to inform any third parties to whom the information has been disclosed of the correction. | 30 days from confirmation |
| 6. | Privacy Officer will keep a record of all enquiries, access requests, corrections and responses. This will comprise a register and file records that will be securely stored in accordance with APP 11. | ongoing |

# APPENDIX C

## Collection Statement Templates

## Collection Statement – Personal Information (i.e. not research information)

[insert organisation name] (ABN/ACN #) respects your privacy. We will only use the information you provide for [insert the primary purposes of collection and any directly related secondary purposes]. We may also disclose your information to [insert names (if known) of third parties to which information will be disclosed and/or (if not known) types of organisation third including party service providers] for these purposes and [insert any other secondary purpose the information may be used for].

Our Privacy Policy, available [here], contains further details regarding how you can access or correct information we hold about you, how you can make a privacy related complaint, how that complaint will be dealt with and the extent to which your information may be disclosed to overseas recipients.

## Collection Statement – Identifiable Research Information

**Background and purpose of the survey/research**

[SPECIFY DETAILS OF THE BACKGROUND OF SURVEY/RESEARCH]

[SPECIFY DETAILS OF THE PURPOSE OF SURVEY/RESEARCH]

**Who is conducting the survey/research?**

**IF ABLE TO REVEAL CLIENT IDENTITY AT THE START:** [NAME OF RESEARCH COMPANY] has been engaged by [CLIENT NAME] to conduct the research. Your contact details were provided to us by [NAME OF CLIENT / OTHER SOURCE].

**IF NOT ABLE TO REVEAL CLIENT IDENTITY AT THE START:** [NAME OF RESEARCH COMPANY] has been engaged by to conduct the research. The identity of the organisation sponsoring this research will be revealed at the end of the survey/ research.

**How long will the survey/ research take?**

This survey/ research should take around XX minutes to complete.

**Is my participation voluntary?**

Participation in this research is voluntary. You can choose not to answer any question. You can decide to stop at any time.

**Is my confidentiality and information privacy protected?**

The information you provide will be treated as private and confidential. Unless you agree otherwise, your information will only be used for the purposes of the research.

At any time during or after the survey, you can ask that the information you provided not be used by [NAME OF RESEARCH COMPANY].

**IF THE CLIENT ORGANISATION WISHES TO OBTAIN IDENTIFIABLE INFORMATION:** We have been asked to pass on [SPECIFY THE TYPE OF INFORMATION] to [NAME OF CLIENT] to be used for [SPECIFY PURPOSE – WHICH MUST NOT BE FOR DIRECT MARKETING]. Do you give permission for us to pass on your information for this purpose?

Yes ☐

No ☐

**IF COLLECTING SENSITIVE INFORMATION:** Please be assured that the information and opinions you provide will be used only for research purposes. While we'd prefer that you answered all the questions, if there is anything that you'd prefer not to answer, that's fine.

**Who do I talk to for further information?**

Should you have any queries regarding the survey/ research, please contact:

- [RESEARCH COMPANY PROJECT MANAGER]

  [RESEARCH COMPANY NAME]

  Tel: (XX) XXXX XXXX

  Email: XXXX

- [CLIENT CONTACT]

  [CLIENT NAME]

  Tel: (XX) XXXX XXXX

  Email: XXXX

**IF PERSON IS LIKELY TO BE RE-CONTACTED TO PARTICIPATE IN FUTURE RESEARCH:**

We do re-contact people from time to time for research projects. With your permission, we will retain your name and contact details for approximately [PERIOD OF TIME] for research purposes only. If at any time you change your mind, you can contact us to request that we remove your name from our list. May we contact you again in the future to invite you to participate in research?

Yes ☐

No ☐

We will not disclose any identifiable research information to a third party for a purpose other than conducting our research unless we have your express prior consent or are required to do so by an Australian law. Information we collect for our research is routinely de-identified and/or destroyed. However, until such time, you have the right to access any information we hold about you. You may request at any time to have any information we hold about you de-identified or destroyed.

Our Privacy Policy is available [here] and contains further details regarding how you can access or correct information we hold about you, how you can make a privacy related complaint, how that complaint will be dealt with and the extent to which your information may be disclosed to overseas recipients. Should you have any questions about our Privacy Policy or any of the above matters, you may contact [insert privacy officer contact details].

# APPENDIX D

## SERVICE LEVEL AGREEMENT (TEMPLATE)

**This Agreement**

**Background**

[insert ADIA agency] (**Agency**) is bound by the Privacy (Market and Social Research) Code as varied from time to time (**Code**), the Privacy Act 1988 (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

The Code, the Privacy Act and the APPs impose strict obligations on the Agency in relation to the collection, use and disclosure of personal information as well obligations in relation to data breaches.

The Notifiable Data Breaches Scheme imposes strict obligations with respect to notifying the Office of the Australian Information Commissioner (**OAIC**) and the individuals whose personal information is involved, where there is a data breach that is likely to result in serious harm.

This privacy agreement (**Agreement)** helps ensure that both our organisations work together to meet those requirements and is designed to help protect the privacy of the people with whom we interact, either directly or indirectly, in the course of any work undertaken.

**Definition of Personal Information.**

"Personal Information" means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

**Obligation to comply with Privacy Laws.**

[insert name of sub-contractor] (**Supplier**) agrees to comply with the terms of this Agreement in the provision of its contracted services (**Services**) to the Agency;

The Supplier must, when it collects, receives, uses, discloses, transfers or otherwise handles Personal Information in the course of performing its obligations under this Agreement:

a) comply with the Privacy Act as though it were a person subject to the Privacy Act and any subordinate legislative instruments or regulations; and
b) comply with any other privacy laws applying to the Supplier or the Agency.

**Permitted use, collection and disclosure.**

The Supplier must:

- collect, use and disclose the Personal Information only as authorised or for the purposes of performing the Services;
- not disclose the Personal Information except:
- to the minimum extent necessary for the purposes of performing the Services;
- as required by Law, subject to the Supplier giving notice to the Agency immediately if it becomes aware that such a disclosure may be required; or
- with the prior written consent of the Agency; and
- ensure that any person to whom Personal Information is disclosed uses, discloses, transfers, retains and otherwise manages such Personal Information consistently with the Supplier's obligations under this Agreement.

The Supplier must:

- not do anything or omit to do anything with the Personal Information that will cause the Agency to breach its obligations under a Privacy Law;
- co-operate with any reasonable requests or directions of the Agency concerning the collection, security, use and disclosure of Personal Information covered by this Agreement, or the rights of individuals to access and correct such Personal Information, except to the extent that compliance with the direction would cause the Supplier to breach their own privacy law obligations;
- provide all assistance as required by the Agency to assist the Agency in complying with its obligations under any Privacy Law;
- if directed by the Agency, implement appropriate data retention and/or data destruction mechanisms in relation to Personal Information;
- where a data breach has occurred that, in the view of the Agency, could reasonably cause serious harm, notify the OAIC of the breach if directed by the Agency to do so; and
- on termination or expiry of this Agreement for any reason, destroy or otherwise deal with any Personal Information collected by or provided to the Supplier as required under this Agreement or otherwise in accordance with the reasonable directions of the Agency.

**Notice requirements.**

When collecting Personal Information from or about an individual which will be disclosed to the Agency, the Supplier must ensure that the individual is provided with a collection notice which complies with APP 5 — Notification of the collection of personal information. For the purposes of this clause, the Agency will supply the collection notice to the Supplier on written request.

**Transborder data flow.**

If the Supplier wishes to transfer or disclose any Personal Information outside of Australia, then the Supplier must, prior to transferring or disclosing any Personal Information, or permitting or allowing access or receipt of any Personal Information:

- provide to the Agency all relevant information relating to the proposed transfer, disclosure, access or receipt, including the country to or in which the Personal Information is proposed to be transferred, disclosed, accessed or received, a detailed description of the Personal Information that is proposed to be transferred, disclosed, accessed or received and the purpose for which such transfer, disclosure, access or receipt is required; and
- obtain the Agency's prior written approval to the transfer, disclosure, access or receipt, which may be granted or withheld at the Agency's sole and absolute discretion. As part of considering whether to give such approval, the Agency may require the Supplier to satisfy the Agency that the arrangements that have been put in place are sufficient to ensure that the handling of Personal Information will at all times be conducted in accordance with the Privacy Act and such other standards or conditions as the Agency may reasonably require.

**Security of Personal Information**

The Supplier must take reasonable technical, administrative, and physical steps to ensure that any Personal Information held or controlled by the Supplier in connection with this Agreement is protected against misuse, loss, unauthorised access, interference, modification or disclosure.

**Reasonable requests**

The Supplier must in respect of any Personal Information held in connection with the Services comply with any reasonable requests or directions issued by the Agency from time to time arising directly from, or in connection with, the exercise of the functions of any officer exercising authority under any Privacy Law.

**Accurate recording and storage of data.**

The Supplier must take all reasonable steps to ensure that Personal Information provided to it in connection with this Agreement is stored or recorded accurately and is not altered or amended except as directed by the Agency.

**Return of Personal Information.**

Except as otherwise required by any applicable law or as otherwise agreed between the parties, the Supplier must return to the Agency all materials in its possession, custody or control containing Personal Information handled in connection with this Agreement in the following circumstances:

- when the Personal Information is no longer required by the Supplier to provide the Services;
- upon demand by the Agency; or
- if required by Law.

**Unauthorised acts**

An unauthorised act in relation to Personal Information occurs if there is any:

- unauthorised disclosure, use, modification or access, or attempted unauthorised disclosure, use, modification or access, or misuse or loss of such Personal Information; or
- act or practice of the Supplier which constitutes an Interference with Privacy of any individual (as that expression is defined in the Privacy Act).

The Supplier must not do, or fail to do, anything which amounts to an unauthorised act in relation to Personal Information.

If the Supplier becomes aware of any unauthorised act in relation to Personal Information, it must:

- notify the Agency as soon as it becomes aware of such unauthorised act;
- take immediate remedial steps to minimise the impact of the unauthorised act on those individuals whose Personal Information is involved;
- promptly provide the Agency with full details of, and assist the Agency in investigating, if requested, the unauthorised act;
- co-operate with the Agency in any investigation in relation to Personal Information;
- use all reasonable efforts to prevent a recurrence of such unauthorised act; and
- comply with any direction from the Agency with respect to remedying such unauthorised act.

**Signed by:**

| **Agency** | **Supplier** |
|---|---|
| Name:_____ | Name:_____ |
| Signature:_____ | Signature:_____ |
| Date:_____ | Date:_____ |

**For further information regarding the APP's and ADIA Privacy Code please contact:**


Sarah Campbell
Chief Executive Officer
ADIA
E: sarah@dataandinsights.com.au

Andrew Maher
Partner, CIE Legal
ADIA Legal Counsel
E: amaher@cielegal.com.au