AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

ADIA Privacy Compliance Committee Annual Report
December 2021

1. The ADIA Privacy Compliance Committee

This report details the activities of the ADIA Privacy Compliance Committee (PCC) from November 2020 to December 2021.

The Privacy Compliance Committee (PCC)

The members of the Privacy Compliance Committee for the reporting year were:

Terry Aulich	Chair
David Vaile	Consumer representative
Szymon Duniec	Industry representative
Andrew Maher	Legal representative
Sarah Campbell	Secretary (CEO ADIA)

The Committee met twice throughout the year and communicated by email and/or phone on issues of interest between meetings. The Terms of Reference for the Privacy Compliance Committee are available on the ADIA website.

2. The Privacy (Market and Social Research) Code – independent Review Report

A copy of the Privacy (Market and Social Research) Code Independent Review Report is available here.

The Committee reviewed the Independent Review of the Privacy (Market and Social Research) Code recommendations led by Professor Peter G Leonard and commissioned by AMSRO (re-branded to the Australian Data and Insights Association /ADIA in April 2021).

Following on from the Review, the following actions have been taken:

a) The Australian Data and Insights Association (ADIA) (formerly the Association of Market and Social Research Organisations (AMSRO)) announced that the Privacy (Market and Social Research) Code 2021 was registered under s 26U of the Privacy Act 1988, by the Australian Information Commissioner Angelene Falk, March 1, 2021.

b) ADIA launched the new Privacy (Market and Social Research) Code 2021 and training resources to members on March 17, 2021.

c) ADIA's Privacy Compliance Committee (PCC) presented an online webinar for members - The New Privacy Code - on March 17, 2021. The webinar provided general training and guidance for members working under the Code and addressed changes in the Code to ensure members understood the new requirements and their obligations. The webinar was attended by over 45 people from 28 member organisations. (The webinar was also made available to all members on-demand.)

d) To meet the annual feedback requirements outlined in Part H of the Privacy (Market and Social Research) Code 2021 - *The Code Administrator will conduct an annual feedback review by making enquiries of Research Organisations in relation to issues or concerns that Research Organisations have experienced in relation to (or within the scope of) operation of this Code during the year in*

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

ADIA Privacy Compliance Committee Annual Report
December 2021

review, including complaints or other concerns of any individual raised with a Research Organisation … - in September 2021, the Association issued member organisations a *Privacy Compliance Checklist* online questionnaire to complete.

Member organisations (n=92) reported the following:

• Two organisations are yet to appoint a privacy officer.

• 69 organisations conduct annual internal privacy training sessions.

• Eight members do not have a privacy policy available to the public.

• 86 organisations have reliable processes and procedures in place for handling inquiries and complaints received from individuals.

• Four organisations received a privacy complaint. These members reported that the complaints related to the following:

- Concern about personal information being provided to clients and other third parties
- Concern as to how personal contact details were obtained
- Concern about information security /risk of data breach.

Members reported that these complaints were addressed swiftly and resolved to the satisfaction of the person making the complaint.

• One member organisation reported a data breach with the matter ongoing to a resolution with the complainant. ADIA's legal counsel and Privacy Officer assisted the member at the time of the data breach and await a final report.

e) Following on from the questionnaire, ADIA is following up with specific members on non-compliance concerns and any gaps identified with current practices.

f) ADIA continues to maintain a register of Privacy Officers from all member companies.

g) ADIA continues to monitor member privacy concerns, complaints or queries as part of its complaints handling procedure. This is managed by Andrew Maher (ADIA Legal) and Sarah Campbell (ADIA CEO and Privacy Manager).

h) The *Privacy Compliance Checklist* questionnaire will be mandated as part of the annual ADIA membership process in 2022.

i) Changes to the global Market and Social Research Industry ISO 20252:2019. This certification is an independently audited ISO standard undertaken by 68 Trust Mark member organisations which includes references and obligation to privacy law. The appended table provides a comparative assessment between the Privacy (Market and Social Research) Code 2021 and ISO 20252:2019 Market, Opinion and Social Research Standard as they apply to an individual person's privacy and data security of personal information (PI).

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

ADIA Privacy Compliance Committee Annual Report
December 2021

The Privacy (Market and Social Research) Code 2021 is based on the Australian Privacy Act and the APPs whereas the ISO 20252:2019 standard references only legislation in general, however does mandate privacy (PI) and data security standards to be achieved in order to comply with ISO 20252: 2019.

Please note: the following documents in relation to the *Privacy Compliance Checklist* questionnaire are appended:

- ADIA member communication (copy)
- The *Privacy Compliance Checklist* (a copy of the online questionnaire)
- ADIA member organisations that completed the questionnaire
- The Privacy Code in relation to ISO 20252:2019

3. Ongoing and on-demand privacy training

To further support our member's compliance to the Privacy (Market and Social Research) Code 2021, ADIA continues to offer a suite of training and guidance materials on best privacy practices and, in August, launched the ADIA Academy – an on-demand online training portal - which hosts the following sessions:

Risk Management - Privacy and Quality Assurance webinars:

- Transitioning to ISO 20252:2019
- Internal Auditor Training ISO 20252:2019
- DIY Information and Data Security Compliance
- Document and Data Control
- Privacy Information Security ISO 20252: Synergies
- The New Privacy Code (2021)

Privacy and Data Security - Compliance Updates

1. Data Protection Laws of Australia
2. Assistance and Access Law of Australia
3. Consumer Rights Laws and the Data and Insights Research Industry
4. The Right to be Forgotten - Erasure.
5. New Zealand Privacy Laws
6. Industrial Manslaughter Laws
7. Anonymity and Pseudonymity
8. Cyber Security for Mobile Devices
9. QR Codes
10. Policies, Policies and more Policies.

4. The Committee reviews and received regular updates on other matters including:

a. The Review of the Australian Privacy Act
b. APEC and OECD developments on privacy matters
c. The activities of the International Data Protection Commissioners
d. ADIA quality assurance activities which have implications for privacy.

Terry Aulich
Chair | ADIA Privacy Compliance Committee
1 December 2021

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

ADIA Privacy Compliance Committee Annual Report
December 2021

Appendix 1:
ADIA Member Communication - Privacy Compliance Checklist

Dear ADIA members,

Privacy Compliance and Reporting under the new Privacy Code 2021.

Please complete by 5 pm Friday 1 October 2021.

Working under Australia's only industry APP Privacy Code, registered by the Office of the Australian Information Commissioner (OAIC), helps mitigate risk for your clients and delivers your organisation greater protection and guidance.

As the Administrator of our new Privacy Code (implemented March 2021), ADIA is required (by law) to monitor member compliance.

- OAIC Report needs to include those member companies (by organisation only) who have completed the self-regulated privacy checklist.

- Under PART H (Monitoring and Reporting) of the Code, we also need to investigate any serious and repeated breaches and systemic issues about code compliance.

- The Privacy Compliance Checklist (see link below) is designed to inform ADIA's reporting duties and help members identify potential gaps in current practices.

- It also provides support where your organisation might need it most with links to privacy resources and specialised training.

- For security purposes, you will need your ADIA login details to access the form. If you do not have a current login, please get in touch with Jennifer@dataandinsights.com.au.

Only one submission per member organisation is required. It does not take long, and if you have any questions, we are here to help.

PLEASE COMPLETE THE CHECKLIST HERE (website address - https://dataandinsights.com.au/member-services/privacy/privacy-compliance-checklist)

Please don't hesitate to contact me via email or on 0460 012 092 should you require anything further.

Kindest regards,
Sarah

Sarah Campbell
CEO I ADIA

Appendix 2: Privacy Compliance Checklist (online questionnaire)

ADIA MEMBER PRIVACY COMPLIANCE CHECKLIST (FOR ONLINE COMPLETION)

ADIA members work under Australia's first and only registered Australian Privacy Principles (APPs) Industry Privacy Code. It is registered (by law) on the OAIC Codes Register.

The Australian Data and Insights Association (ADIA) is required to report annually to the Office of the Australian Information Commissioner (OAIC) on member compliance and their commitment to privacy law and training.

Please answer all of these questions to validate ADIA membership and demonstrate your company commitment to the ADIA Privacy Code obligations.

Should you receive further information please contact ADIA.

E: admin@dataandinsights.com.au

T: 0460 012 092

ADIA Member: _____

Contact: _____

Contact details: _____

- **1. Has your organisation appointed a Privacy Officer? ***

  QUESTION INFORMATION

  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 must have knowledge of privacy legislation and keep abreast of any future changes.

  - ○ Yes ○ No

    Name of Privacy Officer: _____

- **2. Have your employees undergone privacy training over the past 12 months? ***

  QUESTION INFORMATION

  Organisations should ensure staff are familiar with the APPs and the Privacy 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. If you answered no, please see www.dataandinsights.com.au/privacy for further information and tools.

  - ☐ Yes ☐ No

    If yes, when was the training held and how many employees participated?

    Training date/s _____

Number of Employees: _____

- **3. Have you conducted an internal privacy audit over the past 12 months? ***

QUESTION INFORMATION

The purpose of a privacy audit is to analyse an organisations' personal information flow. There is a positive obligation on member organisations to implement practices and systems to ensure organisations comply with the APPs and the Privacy Code.

  - ☐ Yes ☐ No

- **4. Does your organisation have an updated privacy policy available to the public? ***

QUESTION INFORMATION

Ensure your company's privacy policy meets the APP's requirements including how an individual can access and seek correction of personal information, enquire or complain about a breach and if personal information will be disclosed to overseas recipients, in which countries recipients are likely to be located. See Privacy Code APP1 and www.dataandinsights.com.au/privacy

  - ☐ Yes ☐ No

  Please provide Privacy Policy URL: _____

- **5. Are your privacy collection statements up to date and in line with the APP's and Privacy Code? ***

QUESTION INFORMATION

Members are required to update their collection statement/s to comply with the Privacy Code and APP5 to align with the way it uses and discloses personal information. See Privacy Code APP5 and www.dataandinsights.com.au

  - ☐ Yes ☐ No

- **6. Does your organisation conduct Privacy Risk Assessments (PIA) for new projects? ***

QUESTION INFORMATION

A PIA is a process that should be adopted to understand personal information flows and privacy impact in respect of any new project to be undertaken. This will help to manage privacy risks during 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.

Further information in respect of the process for conducting a PIA, including a guidance note and checklist, can be obtained from the OAIC website www.oaic.gov.au/privacy/privacy-resources/privacy-guides

  - ☐ Yes ☐ No

- **7. Does your organisation have a privacy protocol [rules] and information security system in place?** *

QUESTION INFORMATION

Organisations should prepare policies and protocols/rules 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.

  Is your organisation compliant with all of the above?

  - ☐ Yes ☐ No
    - If no, and further information or assistance is required, please contact ADIA at admin@dataandinsights.com.au

Additional resources are available from ADIA:

  - ISO 20252 and Privacy Compliance guideline
  - Information Security

- **8. Does your organisation have an inquiry and complaint program in place?** *

QUESTION INFORMATION

Organisations need to ensure that they implement practices, procedures and systems for handling enquiries and complaints with respect to its compliance with the Privacy Code and the APPs. To ensure the process is fair and consistent, complaints and enquiries should be referred to a single point of contact being the Privacy Officer.

ADIA encourages members to analyse any enquiries and/or complaints overtime to identify trends and improvement opportunities.
My organisation has an inquiry and complaint process:

  - ☐ Yes ☐ No

  Members working under the Privacy Code please refer to www.dataandinsights.com.au/privacyreporting procedures.

- **9. Does your organisation conduct regular privacy audits?** *

QUESTION INFORMATION

Audits should be conducted (outside of your annual ISO 20252 audit) at regular intervals to review what steps your organisation currently takes to ensure personal information is up to date, complete and accurate and in respect of disclosure that it is relevant.

Make sure audits focus on RISKS as identified in the PIA risk assessment as well as measure compliance to policies and protocols. It is imperative that organisations review what steps are currently taken to ensure

personal information collected is protected from misuse, interference, loss and from unauthorised access, modification, or disclosure. See Privacy Code and APP11.

- ☐ Yes ☐ No

  If yes, please provide date of audit: _____

- **10. Is your privacy officer aware they are required to report any potential or actual privacy breaches to ADIA? ***

QUESTION INFORMATION

ADIA member organisations must report to the Code Administrator on the number, nature and outcomes of any serious (or systemic) complaints received about a potential breach. To assist members with this legal requirement ADIA has developed an online guideline and reporting mechanism that can be accessed at www.dataandinsights.com.au/privacy
Members are required to advise ADIA in regard to any serious or systemic complaints received and/or breaches that remain unresolved.

For further details on our data breach process please contact ADIA Secretariat on 0460012 092 or email admin@dataandinsights.com.au or visit the member section at www.dataandinsights.com.au/privacy

- ☐ Yes ☐ No

11. Did your Organisations receive any complaints in FY 21-22 related to privacy?

QUESTION INFORMATION

For the purpose of this question, complaints are broadly defined to include any **issues or** concerns raised about privacy or the collection, use of disclosure of personal information (i.e., not just alleged breaches of the ADIA privacy Code or APPs).

Yes **No**

If yes, your company received complaints:

- How many of these complaints were resolved to the satisfaction of the person who made the complaint?

Insert number: _____

What issues or concerns were raised in the complaints [Select all that apply]?

- Concern as to how personal contact details were obtained
- Concern about personal information being provided to clients and other third parties
- Concern about information security /risk of data breach
- Concern about where and how long your personal data is stored
- Other (please specify): _____

Appendix 3: ADIA Member list – Privacy Compliance Checklist completes – November 2021

Action Market Research	i-Link Research Solutions	Quantum Market Research
Allen + Clarke Pty Ltd	Instinct & Reason	Quirk Research Pty Ltd
ASDF Research	Ipsos and i-view	Research Solutions
Australia Online Research	Jackie Duke Insights	So What Research
Ava Research	JWS Research	Social Research Centre
Bastion Insights	Kantar Consulting Australia	Sprout Research
Beddoes Institute	Kantar Insights	Square Holes
Chitchat Research	Kantar Public	Stable Research
Cint	Landscape Research	Symplicit
CIRCA	Lightspeed	Taverner Research
Cooper Symons & Associates	Luma Research	Telmy
CSBA	Market Access Research and Consulting	The Evolved Group
D&M Research	Market and Communications Research	The Human Network
Data Squirrels	Market Metrics Data Collection	The Insight Centre
DBM Consultants	McNair yellowSquares	The Market Intelligence Co
Dynata	Metrix Consulting	The ORU
Edentify	Myriad Research	The Plug-in
Ekas Marketing Research Services	New Focus	The Purple Corporation
Enable Health Consulting	Omnipoll	The Red Fox Group
Engine	ORIMA Research	The Social Deck
Enhance Research	OzInfo	Thinkfield
EY Sweeney	Painted Dog Research	Think-HQ Pty Ltd
Farron Research	Paper Giant	TKW Research Group
Faster Horses	Parallel Data Research	TRA Melbourne Pty Ltd
Fiftyfive5	Piazza Research	Wallis Social Research
Gallup	Proof Research	Watermelon Research
Growthops	PureProfile	Whereto Research Based Consulting Pty Ltd
Gundabluey	Q&A Market Research Services	Winton Research & Insights Pty Ltd
Hall & Partners	Qualitative Recruitment Australia	YouGov
Hearsay	Quality Online Research	

Appendix 4: ADIA Privacy Code 2021 and ISO 20252:2019 – Comparison Table

OVERVIEW

This document provides a comparative assessment between the ADIA Privacy Code 2021 and ISO 20252: 2019 Market, opinion and social research standard as they apply to an individual person's privacy and data security of personal information (PI).

The ADIA Privacy Code 2021 is based on the Australian Privacy Act and the APPs whereas the ISO 20252 standard references only legislation in general, however does mandate privacy (PI) and data security standards to be achieved in order to comply with ISO 20252: 2019.

The ISO 20252: 2019 Market, opinion and social research standard is undergoing some minor updates in line with changing face of AI technologies however these will not be released until late 2021.

Note terminology variations:

- The ADIA Code refers to a 'research organisation' whereas the ISO 20252 standard refers to the 'service provider'. In the context of this comparative document, they both mean a market research organisation or business.
- The ADIA Code refers to 'personal information' *as any information or opinion (whether true or not) about an individual who is identified or could reasonably be identified*; whereas ISO 20252 refers to 'personal data' *as information relating to a natural living person that can be used to identify an individual*. In the context of this comparative document, it can be assumed they both mean the same.

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
APP 1 Open and transparent personal information	**4.1.2 Confidentiality of research / ANNEX A: Access Panel**
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. Failure may result in a breach of the Privacy Act or the ADIA Privacy Code – grounds for complaint &/or investigation.	**4.1.2.1 General statement.** Information supplied by clients for project purposes shall only be used by service providers in the context for which it was supplied. It shall not be made available to third parties without prior authorization by clients and shall be treated in the strictest confidence in accordance with client requirements. Identifiable participant data are confidential, and all assurances given to participants shall be fulfilled. Where databases or contact lists are provided by third parties (e.g., clients), the service provider shall request that third parties confirm that use of such sources conforms to industry codes. **ISO 20252: Clause 4.3.3 Information security training and awareness** The service provider shall provide training to all staff about handling information appropriately and in a timely manner. The training shall: - be in the context of the information management framework and identified risks; - be delivered annually as a minimum or more frequently if the role requires it;

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
	- include notification to staff regarding their responsibility for safeguarding information; - be appropriate to the risks associated with the information handled by them or to which they have access; - include guidance on how to identify different types of information; and - detail how to ascertain what protection is required for the information they are handling.
If complaints to the research organisation cannot be informally resolved within 30 business days, either the complainant or the research organisation may refer the complaint to ADIA. If not resolved, can escalate to the AOIC. Meeting the annual complaint reporting obligations under Part H (a)of the Code requires research organisations to keep records during the year in a form that will allow them to report to ADIA.	**4.5.2 Client relationship management – client complaints** The service provider shall have a client complaints management process which requires that the complaints shall, at a minimum: — be investigated, documented, and actioned, including a review of the contract and a review for regulatory and industry code compliance or breach notices; and — involve senior management for further action as appropriate and according to the significance of the complaint. The service provider shall ensure that complaints relating to breach of contract, regulation, or industry codes are reviewed at the annual compliance review for improvement opportunities.
Research organisation must also have a clearly expressed and up to date APP privacy policy that provides details about the management of personal information and identifiable research information handled by the organisation. Policy for collection, holding and disclosure of PI for research for the Code 2021 must contain: the kinds of personal information and identifiable research information that is collected and held; - how personal information and identifiable research information is collected and held; - the purposes for which personal information and identifiable research information is held, used and disclosed; - how an individual may access their personal information and identifiable research information and have it corrected; - how an individual may complain about a breach of the APPs and how the complaint will be dealt with; and - 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 Privacy related policies must be available free of charge, in an appropriate form and in the form that an individual or body requests.	**4.1.2.2 Participant reassurance** Invited or recruited participants shall be informed by the service provider that participation is voluntary. The service provider shall ensure that participant reassurance occurs: - during each recruitment or invitation, regarding the types of personal data, proposed uses, and retention and/or reuse of the data to be collected; - during direct data collection (e.g. face-to-face, telephone) regarding confidentiality principles, purposes for which the data may be used, and identity and contact details of the service provider and any subcontractors and/or client(s), as appropriate. **Annex A: Access panel recruitment** The service provider shall inform panel members about the general conditions of participation, including: - privacy and confidentiality; - incentives and rewards policies; - modes of operation (e.g. home use tests, online communities); - general nature of how data are collected from panel members during recruitment or via panel research projects; - how data may be communicated. During recruitment, the service provider shall ensure that potential panel members are informed that cooperation and membership of access panels is voluntary and that, upon request, at any time after recruitment they can be removed from access panels **Annex A 5.2.1 Confidentiality & transparency for access panels** During and after the recruitment process, the service provider shall communicate to and be transparent with panel members about the general purposes of access panels, the modes of operation, and the nature of how data collected from panel members may be used. The service provider shall prepare and make readily available documented privacy statements for panel members during and after recruitment.

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
	The service provider shall only add to the panel people who consent to the terms and conditions of membership and agree to future participation in research projects. The service provider shall explain the types of research to be undertaken to parents or legal guardians in order to gain consent for children or vulnerable persons to be added to panels.
APP 2 Anonymity and pseudonymity	**4.1.2 Confidentiality of research / ANNEX D: Digital observation**
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. 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.	**4.1.2.2 Participant reassurance** Where digital identifiers (e.g., cookies) are used by the service provider during data collection, this shall be communicated to participants including the purpose of the intended identifiers. Whenever geo-location or geo-fencing methods are to be used to collect participant data, the service provider shall make participants aware of this and obtain consent. Where there is no direct contact between the service provider and the participant/s and it is not possible to provide direct assurances, privacy obligations shall still be met. Reasonable precautions shall be taken by the service provider to ensure that participants and observed people (including those who may not be aware they are being observed) are not identified, harmed, or adversely affected as a result of their participation. **Annex D: 3.1.3 Participant safeguards** Where participants have been recruited and have agreed to participate, approaches to participants shall include a brief description of the principles of participant confidentiality, the general research purposes for which the data are to be used, and the name of the service provider, subcontracting agency and/or the client(s), as appropriate. The participants shall be informed that cooperation is voluntary, and participants may withdraw at any time.
APP 3 Collection of solicited personal information	**4.1.2 Confidentiality of research**
Collection of personal information and identifiable research information requires the following standards to be met. Do not collect personal information unless the information is *reasonably necessary* for one or more of its functions or activities. Do not collect identifiable research information unless the information is *reasonably necessary* for one or more research purposes. Only collect personal information and identifiable research information by lawful and fair means. Only collect identifiable research information directly from an individual unless it is unreasonable to impracticable to do so. Only collect personal information about an individual from the individual unless there is consent of the individual to collect the information from a third party, it is required or	**4.1.2.3 Invitation to participate in research projects** The service provider shall provide each potential participant invited to take part in a research project with appropriate information, including: - a general description of the purpose of a project; - the estimated length of their participation time; - a statement of the confidentiality of each participant's responses; - a statement of the anonymity and/or identification of each participant's responses; - the closing date for completed responses (if applicable); - full disclosure of incentive terms and conditions related to the project; - information as to whether the invitation is sent out on behalf of another service provider; and - the opportunity to unsubscribe or opt out of the research activity. Where participants ask for the above details of a project, if the information cannot be shared prior to participation, the service provider shall share these details after participation. **ISO 20252: 2019 Clause 4.1.2.4 Children or vulnerable persons**

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
authorised by law or a court/tribunal order to collect the information from a third party or it is impracticable to do so.	The requirements of 4.1.2.4 regarding the participation of children shall apply.
Collection of sensitive information requires the following standards to be met. Do 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.	
APP 4 Dealing with unsolicited personal information. **This is a new APP giving same protections as solicited information**	
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.	No equivalent in ISO 20252.
APP 5 Notification of the collection of personal information	**ANNEX A Access Panels / ANNEX B Fieldwork / ANNEX D Digital observation**
Collection of personal information *other than research data* standards to be met. An organisation must provide to an individual at or before the time of collecting any personal information (in the form of a privacy collection statement): - 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, 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	**Annex A: Device ID** If device ID is used to remove duplicated participants from samples, the service provider shall use a device ID technology that is capable of supporting geo-location identification, and both duplicate and proxy server identification where possible. The service provider shall be transparent regarding the accuracy of their technique and inform users of its limitations. The service provider shall inform users about data protection requirements associated with the use, transfer, and storage of device IDs. **Annex B: Recording interviews and participant confidentiality** The service provider shall ensure that recordings of groups or depth interview responses are only conducted with consent and only used for the purposes for which the consent was given. Recordings are usually audio, video, or transcripts of typed or uploaded content in online sessions but may include others. The service provider shall ensure that participants are made aware of and have given their consent to recordings as well as any intended uses of the information (e.g., use by third parties) and any transfers of data (e.g., to clients).

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
and if so (and practicable) the countries in which those recipients are located.	The service provider shall ensure that recordings are labelled to identify projects, participants (including by cross-reference to other records) and data collection dates. If recordings are transferred to clients, the service provider shall ensure that clients sign agreements that they will only use recordings internally for research purposes, unless otherwise agreed with the participant. **Annex D Protection of individuals** In order to guarantee as far as possible, the anonymity of the individual persons whose data are to be analysed, possible quotes shall be anonymized during the reporting in such a way that the identification is no longer reasonably possible at any point. As far as possible, the service provider shall ensure that those whose statements or sentiments expressed via social media or those whose behaviour is registered while visiting websites will not experience adverse or direct personal consequences, for example non-consented individually targeted messaging, as a result of the data collection, irrespective of whether the persons concerned have been asked permission for the collection of the specified data. The service provider shall make the client aware of this requirement. Where a combination of data from different sources may lead to the potential identification of participants, reasonable efforts shall be made to protect the anonymity of participants in line with the relevant professional codes of conduct.
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.	
Collection of research data standards to be met. 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: - its identity as the research organisation collecting the information - the position title, telephone number and email address of an ADIA contact who handles privacy related enquires and complaints details. - 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; - any law or court/tribunal that requires the information to be collected; - 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); - the fact that research data collected is routinely de-identified (if this applies) and how long research information is likely to remain identifiable; - the organisations to which information is usually disclosed; - 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; - 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;	**Annex D 3.3. Device monitoring** The service provider shall inform participants of any likely consequences of device monitoring, such as substantial use of device memory, battery power, or impact on internet access, and obtain consent if devices, downloaded software, apps, or other programming can remove, revise, deactivate, or otherwise affect any other software or settings. The service provider shall obtain consent for every install of any device, software, app, or other device monitoring takes place via hardware such as a USB stick or a dongle. The service provider shall obtain consent at regular and reasonable intervals, at least annually, for the continued data The service provider shall adhere to robot instruction files from websites regarding what types of information are permissible to be collected. The service provider shall never use spyware. **Annex A: Cookies & other similar objects** The service provider shall only use or cooperate with third parties that use cookies and other similar objects, including local shared objects (e.g., "flash cookies") and web beacons (including transparent or clear gifs) for legitimate research purposes. These purposes include: - identification of participants or panellists as required for services requested by participants (i.e., to participate in panels and research); - validation and fraud prevention, including legitimate use in device ID technologies; and - tracking activities such as advertising evaluation research and other appropriate research uses. When cookies and other similar objects are used, the service provider shall conform with applicable industry codes, including

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
- the fact the individual can access their identifiable research information prior to it being de-identified or destroyed; - if applicable, that individual may request to have their identifiable research information de-identified or destroyed; and that the research privacy policy explains how an individual may access and correct personal information held about them, 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.	the separation of research and marketing activities. In some jurisdictions, this includes obtaining participant consent to place cookies and other similar objects on devices for the first time and placing cookie notices on any associated websites. The service provider shall inform participants about the nature, presence, and purpose of cookies and other similar objects. This information shall be presented in plain language to allow participants and panellists to give consent.
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.	**A.5 Collecting personal information via Access Panels** The service provider shall actively manage access panels. Such management shall include ongoing communication between the service provider and panel members. At the recruitment stage, the service provider shall obtain agreement from panel members to participate in research projects. The service provider shall ensure that active panel members meet the following criteria: - they are recruited from documented sources; - they have provided appropriate information for initial confirmation of identities; - they have provided profile data at recruitment; and - they have given explicit consent to participate in research according to the terms and conditions of panel membership.
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: - 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; - Individuals have consented to their information being disclosed to the research organisation for research purposes; or - 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.	
APP 6 Use or disclosure of personal information	**4.3.2 Information handling**
Personal information NOT research data standards 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**);	**4.3.2 Information handling** The service provider shall implement a process to determine how different types of information shall be handled according to their associated risks. The process shall identify any types of information which needs to be processed securely and/or to which access needs to be restricted.

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
- 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.	
Identifiable research information standards 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.	
Where research discloses identifiable research information for a research purpose, it must ensure: - Only that part of the information considered necessary for the research purpose is disclosed; - If the research could be achieved using de-identified data, it is de-identified prior to disclosure; and - 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).	
APP 7 Direct marketing	
Research organisations are not permitted to use or disclose identifiable research information about an individual for the purpose of direct marketing.	No equivalent in ISO 20252
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	

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
that they may opt out **and** the individual has not opted out.	
Direct marketing with sensitive information <u>is only permitted with consent</u>.	
Where an individual has been sent direct marketing and he/she: - opts out; - request that personal information not be disclosed to facilitate direct marketing by another; or - request the organisation provide the source of the personal information, then it must give effect to the request within a reasonable period of time.	
APP 8 Cross border disclosure of personal information	**Legal and regulatory requirements**
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.	**Clause 4.8 Legal requirements – as applicable to territorial boundaries** The service provider shall establish, implement and maintain a procedure: - to identify the legal requirements applicable to the activities offered; - to determine how these requirements apply to the activities offered. The service provider shall ensure that these applicable legal requirements are taken into account when offering its services.
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 EU.	
Research organisations will, in certain circumstances, be responsible for a breach committed by the overseas recipient unless it: - 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 - the individual has consented to the disclosure, after having been expressly informed that taking reasonable steps will not apply to the disclosure if consent is provided; or - disclosure is required by court order; or - it is required for a permitted health or safety reason.	
APP 9 Adoption, use or disclosure of Government related identifiers	
Organisations must not adopt, use or disclose a government related identifier (including those of State and Territory	No equivalent in ISO 20252

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
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.	
APP 10 Quality of personal information	**ANNEX A – Access Panel**
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).	**Annex A 5.6.4 updating profile data of panel members** The service provider shall ask panel members to update their profile information at least once every 12 months and allow panellists to update their information (e.g., email address, telephone, address) if they request it at other times. If no changes are needed to profile, the service provider can consider this as an update and confirm it by recording the confirmation date. In this situation, the service provider shall record that panel members have had the opportunity to update their profile. **Annex A 5.1 Panel data** Access panels shall contain a set of profile data of panel members: The service provider shall ensure that active panel members meet the following criteria: - they are recruited from documented sources; - they have provided appropriate information for initial confirmation of identities; - they have provided profile data at recruitment; and - they have given explicit consent to participate in research according to the terms and conditions of panel membership. In order to remain an active panel member, the service provider shall ensure that at least one of the following criteria is met: - the panel member has completed at least one research project, if requested, within the last 12 months, including qualified completion, being terminated due to not qualifying, or being terminated due to quotas being full; - the panel member has updated their profile data within the last 12 months.
APP 11 Security of personal information	**4.3 Information Security**
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	**4.3.1 Information security risk framework** The service provider shall identify the security risks associated with the information they process and implement an information security management framework to prevent the unauthorised access, use, modification or destruction of the information. This framework shall be appropriate to the risks identified and shall apply to the collection, receipt, storage, transfer and deletion of

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
additional measures, which are reasonable in the circumstances, to protect against computer attacks and other interferences.	information. This framework shall be inclusive of all formats and locations in which the information may be held. **4.3.3 Information security controls** The service provider shall implement a process to determine how different types of information shall be handled according to their associated risks. The process shall identify any types of information which needs to be processed securely and/or to which access needs to be restricted.
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 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.	**4.1.3.3 Records management** The extent and nature of records management, including maintaining, archiving, and destruction of records for research activities undertaken by the service provider, shall be: - controlled in a secure manner - protected from loss of confidentiality, privacy, and security - protected from improper use and loss of integrity
Research organisations must also comply with the following additional obligations to destroy or de-identify identifiable research information: - To destroy or de-identify identifiable research information once it is no longer necessary for research purposes; - 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; - 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 - Take reasonable steps to ensure that any identifiable research information it discloses will be used in accordance with the Code, protected by the recipient from misuse, interference, loss, unauthorised access, modification or disclosure; and 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.	**ISO 20252 Clause 4.8 Legal Requirements** The service provider shall establish, implement and maintain a procedure: - to identify the legal requirements applicable to the activities offered; - to determine how these requirements apply to the activities offered. The service provider shall ensure that these applicable legal requirements are taken into account when offering its services.
APP 12 Access to personal information	**ANNEX A: Access panel**
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	**Annex A 5.6.3 Panel data maintenance** The service provider shall interact with panel members at least once every 12 months, whether as part of research project participation, updating of profile data, or otherwise. Such interaction by the service provider shall entail two-way communication between the service provider and panel members and shall be documented.
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);	

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
- 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.	
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.	
APP 13 Correction of personal information	**ANNEX A: Access Panel**
Correction standards. If an organisation holds personal information or identifiable research information other than research data (such as contact details or research status) 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: - 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 - If requested, associate a statement with the information that the individual believes the information is inaccurate, out of date, incomplete, irrelevant or misleading.	**Annex A: 4.3.1 Quality of data – de-duplication** The service provider shall take reasonable efforts to remove duplicate participants, some of whom may result from the use of multiple sources (e.g., panels, social networks, river sample) to develop samples.
Request for destruction or de-identification of personal information standards. Research organisations must accept and act on requests for identifiable research information to be destroyed or de-identified, except in the following circumstances: - The request is frivolous or vexations (e.g., it is trivial and made for amusements sake, is being made to pursue some other grievance against the organisation, is a repeated request or is made principally to create inconvenience); - Destruction or de-identification would have an unreasonable impact on the privacy of other individuals; - The research organisation is contractually obliged to retain the information; and - Destruction or de-identification would pose a health or safety risk, prejudice negotiations with the individual, be unlawful, is required to be retained by a law or	**Annex A.5.4 Request to unsubscribe or opt out of the access panel** The service provider shall provide panel members with a straightforward method for removal from access panels if they choose. The service provider shall complete a request for removal as soon as is practical but no later than 30 days after the request. The service provider shall not select such panel members for future research studies from any relevant access panels unless new acceptances are obtained by the service provider from former panel members to recommence participation in future recruitments or research.

ADIA Privacy Code 2021	ISO 20252: 2019 CORE Information + ANNEXES
court/tribunal order or prejudice a law enforcement related activity.	
Notification standards. 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.	No equivalent in ISO 20252
Refusal standards. 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.	No equivalent in ISO 20252
Request to associate a statement standards. 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.	No equivalent in ISO 20252
Dealing with requests standards. 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.	No equivalent in ISO 20252