AMSRO

Association of Market and Social Research Organisations

Privacy
(Market and Social Research)
Code 2021

Commencement Date: 22 March 2021

www.amsro.com.au

Contents

Preliminary P. 3

A. PREAMBLE P. 4

B. OBJECTIVES P. 6

C. ELIGIBILITY AND COVERAGE [S26C(3)] P. 7

D. TERMINOLOGY P. 8

E. HOW THE AUSTRALIAN PRIVACY PRINCIPLES APPLY TO MARKET AND SOCIAL RESEARCH

Transparency of management P. 13

APP 1 & APP 2

Collection of personal information P. 15

APP 3, APP 4 & APP 5

Dealing with personal information P. 21

APP 6, APP 7, APP 8 & APP 9

Integrity of personal information P. 28

APP 10 & APP 11

Access to, and correction of, personal information P. 30

APP 12 & APP 13

F. GOVERNANCE [CDGL Pt 3] P. 37

G. REVIEW [CDGL Pt 6] P. 38

H. MONITORING AND REPORTING P. 39

Privacy (Market and Social Research) Code 2021

Annotated version, including Explanatory Notes

Explanatory Note:
This version includes annotations, which are in italics, prefaced with 'Explanatory Note and/or Guidance'. These explanations do not form part of this Code, and will remain only in an annotated version.
Text in normal brackets like (this) form part of this Code.
Only Parts D, E & H (some clauses only) of this Code are 'registered' as a Code under Part IIIB of the Privacy Act 1988. These represent obligations (and the relevant definitions), breach of which by a Research Organisation constitutes an 'interference with privacy'.
The other parts of this Code (Part A, Preamble; Part B, Objectives; Part C; Eligibility and Coverage; Part F; Code Governance; Part G, Review, and the remaining clauses of Part H are necessary operational provisions and/or 'context' to make the Code a self-contained document meaningful to the industry and to consumers, and capable of practical implementation.
[Text in italics and in square brackets like [this] is included in this version to explain how provisions of the Code relate to requirements of the Act; e.g., [s16A; APP 1.3] or to the Information Commissioner's Code Development Guidelines; e.g., [CDGL 2.1]. Text in square brackets does not form part of the Code and will be removed from the published version.

Preliminary

1. Name of APP code

This APP code is the Privacy (Market and Social Research) Code 2021. It replaces the *Privacy (Market and Social Research) Code 2014*.

2. Commencement

This APP code comes into force under the *Privacy Act 1988* (**Privacy Act**) when it is included on the Codes Register kept under s26U(1) of that Act and will remain in force until it is repealed. The *Privacy (Market and Social Research) Code 2014* will cease to operate when this APP code comes into force.

3. Authority

This APP code is a 'registered APP code' under s26B(1) of the Privacy Act, and a legislative instrument, once it is included on the Codes Register kept under subsection 26U(1) of that Act and is in force.

4. Entities bound by this APP code

All members of the Association of Market and Social Research Organisations ABN 20 107 667 398 who are an organisation covered by the Privacy Act (including because they have opted in under s 6EA of that Act) are bound by this APP Code. If

an organisation covered by the Privacy Act ceases to be a member of AMSRO, they will still be liable under this APP code for acts and practices that breach this APP code and that occurred while they were an AMSRO member.

A. PREAMBLE

a. The Association of Market and Social Research Organisations (**AMSRO**) is the national industry body of market and social research, data and insights organisations. AMSRO's primary objective is to protect and promote the research, data and insights sector so that this sector can continue its important contribution to Australia's economic, social and political wellbeing. In AMSRO's view, the long-term success of the sector depends upon the willing cooperation of the public and business community, which is based upon confidence that the work of the sector is carried out honestly, objectively and without unwelcome intrusion or disadvantage to participants.

b. AMSRO decided on its own initiative to develop this APP Code under Part IIIB of the Privacy Act.[1]

   This Code replaces the Market and Social Research Privacy Code 2014.

c. Part E of this Code sets out how the Australian Privacy Principles (**APPs**) in the Privacy Act are to be applied and complied with by AMSRO members in relation to the collection, retention, use and disclosure of personal information about the subjects of and participants in **Market and Social Research** (referred to in this Code as **identifiable research information**). The subjects/participants are any individuals about or from whom any information is sought, collected, retained, used and/or disclosed by a Research Organisation for the purposes of research (**research subjects**). The provisions of this Code seek to give effect to the APPs in a manner that is tailored to the research context while providing the public and business community with the assurances needed to encourage informed and willing participation in Market and Social Research activities. This Code acknowledges and draws on relevant Guidelines published by the Office of the Australian Information Commissioner (OAIC).[2]

d. This Code imposes some *additional* requirements to the requirements of the APPs. These obligations reflect the fact that participation by research subjects in Market and Social Research as carried out by AMSRO members is always voluntary; that market and social researchers are generally not interested in making use of the identity of research participants; and that they use and disclose the information collected only for research purposes.

e. In some cases, the editing of the APPs in Part E simply deletes wording that is not applicable, such as where relevant APPs apply only to 'agencies' or where relevant APPs govern practices, such as direct marketing, which are incompatible with Market and Social Research as carried out by AMSRO members.

---

[1] The Privacy Act is available at http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act.

[2] In particular: OAIC, Guidelines for developing codes (available at https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-for-developing-codes/) and OAIC, Australian Privacy Principles (APP) Guidelines (available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines).

f. It is not intended that this APP Code will cover acts and practices that are otherwise exempt under section 7B of the Privacy Act.

g. This Code includes (under APP 1.2 in Part E and in Part H) obligations relating to the internal handling of complaints and referral to the Commissioner. It includes standardised provisions for the reporting of complaints to the Code Administrator and to the Commissioner. These are additional to the 'default' complaint-handling provisions of the Privacy Act (Part V), which apply to any complaints about breaches of this Code.

h. This Code is administered by the AMSRO Secretariat, under direction of the AMSRO Board[3]. It will remain in force whilst registered but is subject to periodic independent review by an Independent Code Reviewer, appointed afresh for each review (see Part G).

i. Significant penalties apply for breaches of the APPs. In the case of organisations found to have committed serious or repeated breaches, penalties can be up to $2.1 million (as at August 2020).

j. The Notifiable Data Breaches (**NDB**) scheme requires organisations covered by the Privacy Act 1988 to notify the Australian Information Commissioner and affected individuals about data breaches that are likely to cause serious harm. An 'eligible data breach' arises when the following three criteria are satisfied: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this is likely to result in serious harm to one or more individuals to whom the information relates, and the entity has not been able to prevent the likely risk of serious harm with remedial action. Examples of a data breach include when a device containing customers' personal information is lost or stolen, a database containing personal information is hacked, or personal information is mistakenly provided to the wrong person. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm. Examples may include identity theft, significant financial loss by the individual, threats to an individual's physical safety, loss of business or employment opportunities, humiliation, damage to reputation or relationships, and workplace or social bullying or marginalisation.

   If an entity only has reason to suspect that there may have been a serious breach, it must take all reasonable steps to complete the assessment within 30 calendar days after the day on which the entity becomes aware of the grounds that cause it to suspect an eligible breach had occurred. It must move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, an entity becomes aware that there are reasonable grounds to believe an eligible data breach has occurred, then the entity must notify the Commissioner and the affected individuals. The NDB scheme provides three options for notifying individuals, and the notification to individuals should generally include the contents of the entity's statement to the Commissioner.

[3] AMSRO is the entity that is the Code Administrator – see Part F.

B. OBJECTIVES

The aims of this Code include:

i. To set out how the Australian Privacy Principles (**APPs**) in the Privacy Act are to be applied and complied with by AMSRO members in the conduct of market and social research;

ii. To facilitate the protection of research information about identifiable individuals being the participants or subjects of Market and Social Research as provided by, or held in relation to, those participants or those subjects; and

iii. To enable quality research to be carried out so as to provide accurate information to government, commercial and not-for-profit organisations to support their decision-making processes.

C. ELIGIBILITY AND COVERAGE [S26C(3)]

a. Subscription to this Code is a requirement of AMSRO membership, regardless of a Research Organisation's size or annual turnover. A current list of AMSRO members, and therefore of APP entities bound by this Code, is maintained at http://www.amsro.com.au.

Explanatory Note:
*Some AMSRO member organisations will have an annual turnover of less than $3 million but AMSRO expects that none of its members will qualify for the Small Business Operator (**SBO**) exemption because the nature of at least part of their business is to 'provide a ....service ... to collect personal information about another individual from anyone else ...'.*[4]
This, and any work as a contractor to a Commonwealth agency[5]*, disqualifies smaller businesses from claiming the SBO exemption (s6(4)).*
AMSRO requires any member organisation that considers itself eligible for the SBO exemption to elect to be subject to the Act by registering with the Commissioner (pursuant to s6EA of the Privacy Act).

b. Organisations that are not members of AMSRO are not eligible to subscribe to this Code.

c. Eligibility for AMSRO membership is open to Research Organisations provided that the Research Organisation meets and complies with AMSRO's Articles of Association.

d. AMSRO membership, and thus subscription to this Code, is voluntary. However, this Code is binding on those Research Organisations that are AMSRO members.

e. Any personal information about individuals that is handled by AMSRO members outside the context of market and social research, such as marketing lists and contact details for clients and service providers, and staff recruitment records, is not subject to this Code but will be governed by the Privacy Act.

[4] Privacy Act, section 6D(4)(d).
[5] Privacy Act, section 6D(4)(e).

D. TERMINOLOGY

Many terms used in this Code have their meaning defined in the Privacy Act. Further explanation of some of those terms in the ***Market and Social Research*** context is required, and the meaning of other key terms is also set out in this section:

Breach of this Code means a breach of any obligation on ***Research Organisations*** under Parts E and H of this Code (also taking account of the terminology in Part D).

Explanatory Note:
'Breach of this Code' is not applicable to the other parts of this Code which relate to preamble (Part A); objectives (Part B); eligibility and coverage (Part C); governance (Part F) and review (Part G).

Client means an organisation, agency, etc., that requests, commissions or subscribes to a given ***Market and Social Research*** project; i.e. the ultimate beneficiary of the research findings.

This Code means this Market and Social Research Privacy Code (an APP Code under the Privacy Act).

The Code Administrator *is AMSRO*. See F(a).

Collection of identifiable research information means gathering, acquiring or obtaining ***identifiable research information*** from any source, by any means, for inclusion in a record.

Explanatory Note:
Collection may be directly from an individual or indirectly from another person or organisation. In practical terms, collection in ***Market and Social Research*** *is likely to include, but not be limited to, the recording of responses given in research (e.g. telephone surveys, central location surveys), the receipt of self-completion questionnaires (e.g. postal questionnaires, online questionnaires), the audio and/or video recording of group discussions or interviews, the recording of contact details of potential research participants (e.g. panels), observation of behaviour and the receipt of customer information from clients.*

Commissioner means the person who has functions and powers under the Privacy Act 1988.

Contact details means a record of identifying information such as names, companies, position titles, addresses and phone numbers, collected and retained in order to contact individuals in a research sample.

De-identification means a process of ensuring that identifiable research information is rendered permanently non-identifiable; i.e., without retaining a means by which the information could be reasonably re-identified.[6]

Explanatory Note:

De-identification is intended to be a permanent and irreversible process. Other techniques, such as the removal of identifiers, may be used to make identification more difficult but if there remains a reasonable possibility of identification, data has not been 'de-identified'. Other than by aggregation of information, it may never be possible to guarantee de-identification, and whether any particular approach to de-identification meets the standard required in the context of the Privacy Act will be a matter (to be) decided on the facts.

Direct marketing involves the use and/or disclosure of identifiable research information to communicate directly with an individual to promote goods and services, whether through voice communications, electronic messaging, mail, email, social media channels and/or online or mobile advertising.[7]

Disclosure of identifiable research information means ***identifiable research information*** becoming known outside an organisation, whether or not it is physically or electronically released or transferred (e.g., including by telling, showing or displaying to another person). Disclosure may be deliberate, or inadvertent (such as a data breach). In assessing whether an individual is reasonably identifiable, regard is to be had to all information reasonably available to an entity, such as other data points and data sources that might be used to infer or confirm the identity of a purportedly non-identifiable person. Accordingly, although information as disclosed by an organisation may not appear to be identifying of any individual, that information may be personal information about an identifiable individual when in the hands of a recipient (even if the information was otherwise not personal information about an individual when in the hands of a discloser). In this circumstance the disclosing entity must treat the disclosure as a disclosure of personal information about an individual, even though the individual is not identified within the information disclosed.[8]

---

[6] See further: OAIC, De-identification and the Privacy Act, March 2018, available at https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/; also OAIC, Guide to data analytics and the Australian Privacy Principles, March 2018, available at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/; in particular, at section 1.6. As noted in OAIC, De-identification and the Privacy Act, "The Privacy Act does not require de-identification to remove the risk of re-identification entirely. Rather, those sharing or releasing data must mitigate the risk until it is very low. That is, until there is no reasonable likelihood of re-identification occurring. As part of this, the entity should consider all relevant risks that may impact on the likelihood of re-identification, including the risk of attribute disclosure, and the risk of spontaneous recognition. Entities should also consider the gravity of any harm that could arise from re-identification."

[7] See paragraphs [7.9] to 7.12] of Chapter 7: APP 7 – Dealing with unsolicited personal information, of OAIC, Australian Privacy Principles Guidelines, rev July 2019, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing/.

[8] See further: OAIC, What is personal information?, May 2017, available at https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/.

Genuine research concerns mean where the ***Research Organisation*** has valid reasons to expect that the purpose of the ***Market and Social Research*** exercise would otherwise be defeated.

Explanatory Note:
Examples of 'genuine research concerns' include:

- *where bias due to non-response (or research opt-outs) may materially affect the information obtained in the research exercise;*
- *where significant public interest lies in achieving high response rates;*
- *where the research is a genuine study of non-response or research opt-outs;*
- *where prior knowledge of the likelihood of being re-contacted may materially affect the information obtained; or*
- *where the validity of a longitudinal or ongoing research exercise may be compromised.*

Identifiable research information means personal information about survey participants, respondents or subjects to which this Code applies. It includes ***contact details***, ***research status*** and ***research data***. It does not include any unsolicited information.

Explanatory Note:
Personal information is defined in the Privacy Act as '... information or an opinion about an identified individual, or an individual who is reasonably identifiable... .'
Market and Social Research *generally involves three types of* ***identifiable research information****:* ***contact details***, ***research status*** *and* ***research data****.*
Identifiable information in research is likely to include, but is not limited to:
interview records awaiting validation or for use in longitudinal research; audio or video recordings of research (research data); and lists of actual or potential research participants (e.g., recruitment databases, panels, customer information) (contact details and research status).
Identifiable information in research may also include information that is not collected by means of direct questioning but by techniques such as observation or remote recording of customer behaviour.
Any unsolicited information should be dealt with in accordance with APP 4.[9]

Market and Social Research means consent-based investigation of the behaviour, needs, attitudes, opinions, motivations or other characteristics of a whole population or a particular part of a population in order to provide accurate and timely information to clients (government, commercial and not-for-profit organisations) about issues relevant to their activities to support their decision-making processes.

[9] See Chapter 4: APP 4 – Dealing with unsolicited personal information, of OAIC, Australian Privacy Principles Guidelines, rev July 2019, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information/.

Explanatory Note:
*The process of **Market and Social Research** includes specifying the information required to achieve the specific research needs of the client, designing the method for collecting information, managing and implementing the data collection process, analysing the results, and communicating the findings and their implications to clients.*
Methods of collecting information in Market and Social Research include postal or mail surveys, e-mail surveys, internet surveys, telephone surveys, door-to-door surveys, central location (e.g. shopping centre) surveys, observational techniques, desk research, and the recruitment and conduct of group discussions (e.g. focus groups), in-depth interviews and series of interviews with online panels. Market and Social Research is always consent-based – any mandatory provision of personal information from and about survey participants, respondents or subjects is not Market and Social Research within the scope of this Code.
Market and Social Research differs from other forms of information gathering in that the information is not used or disclosed either to support measures or decisions with respect to the particular individual without the express consent of that individual, or in a manner that could result in any serious consequence (including substantial damage or distress) for the particular individual.

Research data means a record of the responses provided by individuals participating in ***Market and Social Research*** at the time of collection in order to obtain a representation of a population's or sub-population's behaviour, needs, attitudes, opinions and motivations at a given point in time.

Research information privacy policy means the APP policy that a ***Research Organisation*** develops, maintains and publishes to comply with APP 1 in relation to identifiable research information.

Research Organisation means an organisation (or that part of an organisation) that is a member of AMSRO and that carries out or acts as a consultant or subcontractor in relation to ***Market and Social Research***, or offers their services or the services of others to do so.

Research Purpose means the handling of information in order to carry out any function considered essential to the conduct of a ***Market and Social Research*** project or communication of the results of a Market and Social Research project.

Explanatory Note:
*In practical terms, **Research Purpose** includes handling information in order to conduct analysis, maintain its accuracy, draw a research sample, carry out quality control, note the willingness or unwillingness of an individual to be contacted in relation to future **Market and Social Research**, assist in the resolution of a problem that has come to light during a Market and Social Research activity, report research results or conduct further Market and Social Research.*

Research status means information in relation to whether or not an individual has been contacted or has participated in a ***Market and Social Research*** exercise but does not include research data.

Explanatory Note:
Research status *information is likely to take the form of a list containing customers' contact details, forwarded from a client organisation to a* ***Research Organisation*** *for research sampling, that also conveys or contains information about actual contact with those individuals or their participation in* ***Market and Social Research****.*

Research subject means an individual about whom identifiable research information is collected in the course of ***Market and Social Research***. *Research subjects* may be referred to as participants or respondents and may include another individual about whom a subject is providing information.

Unsolicited information means identifiable research information that a ***Research Organisation*** has taken no active steps to collect.[10]

Explanatory Note:
Most identifiable research information handled in the context of ***Market and Social Research*** *is solicited, in that it has been gathered systematically. However, at times researchers may receive information that they have not asked to receive. This information may be offered voluntarily by research subjects or may be captured as a by-product of other activities; for example, electronic recordings or client-provided lists that contain more information than is necessary to conduct the research.*

[10] See further: para. [4.5]-[4.9] of Chapter 4: APP 4 – Dealing with unsolicited personal information, of OAIC, Australian Privacy Principles Guidelines, rev July 2019, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information/.

E. HOW THE AUSTRALIAN PRIVACY PRINCIPLES APPLY TO MARKET AND SOCIAL RESEARCH

Explanatory Note:
This Part contains a customised set of Australian Privacy Principles for the Market and Social Research context. They show how the Australian Privacy Principles in the Privacy Act 1988 are to be applied or complied with by Research Organisations in relation to identifiable research information.

Transparency of management

Australian Privacy Principle 1: Open and transparent management of personal information (as customised for the purposes of this Code)

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles

1.2 When handling identifiable research information, Research Organisations must take such steps as are reasonable in the circumstances to implement practices, procedures and systems[11] relating to the Research Organisation's functions or activities to ensure that:

(a) the Research Organisation complies with the Australian Privacy Principles and this Code; and

(b) the Research Organisation can deal with inquiries or complaints from individuals about the Research Organisation's compliance with this Code.

Explanatory Note:
Grounds for complaints
A breach of the obligations on Research Organisations under Parts E and H of this Code is an 'interference with privacy', which is grounds for complaint and/or investigation under the Act. Research Organisations must ensure that they have in place, and publicly available, procedures for dealing with complaints about alleged breaches of this Code from inception to satisfaction or determination, which are available to any individual (irrespective of nationality or place of residence) about whom identifiable research information is held.

- *If complaints cannot be informally resolved between the complainant and the Research Organisation within 30 business days, either the complainant or the Research Organisation may refer the complaint to the Code Administrator.*

[11] See examples of practices, processes and procedures in paragraph 1.7 of OAIC, Australian Privacy Principles Guidelines, rev July 2019, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines.

- *If complaints cannot be resolved to the satisfaction of the complainant or Research Organisation by the Code Administrator either informally or within a formal industry-based complaint-handling process, either the complainant or the Research Organisation may refer the complaint to the Commissioner.*

In order to meet the annual complaint-reporting obligation of this Code (Part H (a)), Research Organisations will need to keep records during the year in a form that will allow them to report to the Code Administrator.

APP Privacy Policy

1.3 A Research Organisation must have a clearly expressed and up-to-date research information privacy policy about the management of identifiable research information by the organisation.

1.4 Without limiting subclause 1.3, the research information privacy policy must contain the following information:

(a) the kinds of identifiable research information that the organisation collects and holds;

(b) how the organisation collects and holds identifiable research information;

(c) the research purposes for which the organisation collects, holds, uses and discloses identifiable research information;

(d) how an individual may access identifiable research information about the individual that is held by the organisation and seek the correction of such information;

(e) how an individual may complain about a breach of this Code, and how the organisation will deal with such a complaint;

(f) whether the organisation is likely to disclose identifiable research information to overseas recipients;

(g) if the organisation is likely to disclose identifiable research information to overseas recipients, and the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of privacy policy

1.5 A Research Organisation must take such steps as are reasonable in the circumstances to make its research information privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

1.6 If a person or body requests a copy of the research information privacy policy of a Research Organisation in a particular form, the organisation must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Explanatory Note:
A Research Organisation must have its own research information privacy policy, and should reference this Code, and provide links to it. A Research Organisation should take reasonable steps to make available copies both of its own policy and of this Code and any relevant explanatory material on request, free of charge and in an accessible way, including on its internet site.

Australian Privacy Principle 2: Anonymity and pseudonymity (as customised for the purposes of this Code)

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with a Research Organisation in the context of Market and Social Research.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the Research Organisation is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the Research Organisation to deal with individuals who have not identified themselves or who have used a pseudonym.

Explanatory Note:
Wherever practicable, Research Organisations will not collect identifying details such as names, but in many research activities, contact details will have been provided for the sample population, and it will not be practicable to comply fully with this principle. In other research activities, the research data (including IP addresses in the case of online surveys) may potentially allow for identification, even without contact details. Again, in these circumstances it will not be practicable to comply with the principle, although the chances and risk of re-identification may be remote.

Collection of personal information

Australian Privacy Principle 3: Collection of solicited personal information (as customised for the purposes of this Code)

Personal information other than sensitive information

3.1 Not applicable (agencies only).

3.2 In the conduct of Market and Social Research, a Research Organisation must not collect identifiable research information (other than sensitive information) unless the information is reasonably necessary for that research.

Sensitive information

3.3 A Research Organisation may only collect sensitive information (whether from an individual or from a third party) where the individual has consented, and the information is reasonably necessary for a research purpose, or if the collection is required by an Australian law or a court/tribunal order.

Explanatory Note:
The Privacy Act allows for sensitive information to be collected if required by Australian law or a court/tribunal order, although AMSRO cannot envisage any circumstances where this would apply in a research context.

Means of collection

3.5 In the conduct of Market and Social Research, a Research Organisation must collect identifiable research information by lawful and fair means only.

Explanatory Note:
A 'fair means' of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive. It would usually be unfair to collect personal information covertly without the knowledge of the individual. A collection may be unfair if it disrespects cultural differences or if there is misrepresentation as to the purpose or effect of collection, or the consequences for the individual of not providing the requested information.[12]

3.6 In the conduct of Market and Social Research, a Research Organisation must collect identifiable research information about an individual only from the individual unless it is unreasonable or impracticable to do so.

Explanatory Note:
If it is reasonable and practicable to do so, a Research Organisation should collect identifiable research information directly from the individual concerned, rather than from third parties.

Solicited personal information

3.7 This principle applies to the collection of identifiable research information that is solicited by a Research Organisation.

[12] See para [3.62]-[3.63] of Chapter 3: APP 3 – Dealing with unsolicited personal information, of OAIC, Australian Privacy Principles Guidelines, rev July 2019, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information/.

Explanatory Note:
Most identifiable research information handled in the context of Market and Social Research is solicited.

Australian Privacy Principle 4: Dealing with unsolicited personal information (as customised for the purposes of this Code)

4.1 If:

(a) a Research Organisation receives identifiable research information; and

(b) the Research Organisation did not solicit the information;

then the Research Organisation must, within a reasonable period after receiving the information, determine whether or not the Research Organisation could have collected the information under APP 3 if the Research Organisation had solicited the information.

4.2 The Research Organisation may use or disclose the identifiable research information for the purposes of making the determination under subclause 4.1.

4.3 If the Research Organisation determines that it could not have collected the identifiable research information, it must, as soon as practicable, but only if it is lawful and reasonable to do so, destroy the information or ensure that it is de-identified.

4.4 If subclause 4.3 does not apply in relation to the identifiable research information, then APPs 5-13 apply in relation to the information as if the Research Organisation had collected the information under APP 3.

Explanatory Note:
Most identifiable research information handled in the context of Market and Social Research is solicited. However, if any unsolicited information is received by a Research Organisation, it must, depending on the circumstances, be destroyed, de-identified or handled in accordance with the APPs.

Australian Privacy Principle 5: Notification of the collection of personal information (as customised for the purposes of this Code)

5.1 At or before the time or, if that is not practicable, as soon as practicable after, a Research Organisation collects identifiable research information about an individual, the organisation must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the Research Organisation;

(b) if:

(i) the Research Organisation collects the identifiable research information from someone other than the individual; or

(ii) the individual may not be aware that the Research Organisation has collected the identifiable research information;

then the fact that the Research Organisation so collects, or has collected, the identifiable research information and the circumstances of that collection;

(c) not applicable;

(d) the purposes for which the Research Organisation collects the identifiable research information;

(e) the main consequences (if any) for the individual if all or some of the identifiable research information is not collected by the Research Organisation;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the Research Organisation usually discloses identifiable research information of the kind collected by the Research Organisation;

(g) that the research information privacy policy of the Research Organisation contains information about how the individual may access the identifiable research information about the individual that is held by the entity and seek the correction of such information;

(h) that the research information privacy policy of the Research Organisation contains information about how the individual may complain about a breach of this Code, and how the entity will deal with such a complaint;

(i) whether the Research Organisation is likely to disclose the identifiable research information to overseas recipients;

(j) if the Research Organisation is likely to disclose the identifiable research information to overseas recipients, then the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Explanatory Note:
In the conduct of Market and Social Research, it should always be possible to make respondents aware of these matters at the time of collection of the identifiable research information (i.e. it should never be necessary to delay notification).
In the circumstances of Market and Social Research, it should always be reasonable to convey all of the matters.
In relation to matter 5.2(a):
The identity and contact details of the Research Organisation should always be provided. Note that the Privacy Act allows affected individuals to contact an entity in multiple ways, and each Research Organisation should not be overly prescriptive or limiting as to the only ways in which the Research Organisation will accept communications. Participating individuals should also be informed as to with whom they may raise queries or concerns. An appropriate contact point may be described by function (i.e. the Privacy Officer) or by name or both.
In relation to matter (b)(i): Collection of information for research from third parties:
If a Research Organisation collects identifiable research information relating to an individual from a third party (such as another householder or member of the family), it should take reasonable steps to ensure that the individual is, or has been, made aware of the matters listed in APP 5.2 and that the individual may obtain further information in relation to this from the Research Organisation.

If a Research Organisation collects personal information other than research data (such as contact details) from a third party (such as a client or list provider), it should take reasonable steps to, ensure that the individual is, or has been, made aware of the matters listed in APP 5.2, and ensure that at least one of the following applies:

i. *the purpose for which the information was originally collected is related to the Market and Social Research to be conducted and the individual would reasonably expect to be contacted to be invited to participate in such research [spirit of APP 6.2(a)]; or*
ii. *all individuals who are identifiable have consented to their identifiable information being released, either specifically for research purposes or generally for a range of purposes related to research [spirit of APP 6.1(a)]; or*
iii. *a readily accessible means exists by which an individual who is identifiable can withdraw his or her consent to being included on the provided list, and this fact is made known to any person who is contacted at the time of such contact [spirit of APP 7.2].*

In relation to this obligation, for example, the individual may be, or have been, made aware by the third party that their personal information may be disclosed to Research Organisations to be used for research purposes, and that the individual may obtain further information in relation to this from the third party. Alternatively, at the time of any contact, the individual may be made aware that the Research Organisation has collected his or her identifiable research information from the third party for research purposes.
***In relation to matter (c)**, at the time of approval there are no laws to compel individuals to provide information for Market and Social Research (other than those empowering the Australian Bureau of Statistics and Australian Institute of Health and Welfare, which are bound by the APPs, not by this Code). If such a situation arose, then the Code would need to be revised to include 'lawful authority' as a matter to be notified.*

In relation to matters (d), (e) and (f), *Research Organisations should explain in their collection notice:*

i. *the fact that the personal information collected will be used only for Market and Social Research purposes and that no other use will be made of the information, either during the research or afterward, subject to the exceptions explained below in relation to APP 6 (which are a subset of those allowed by the Act), and*
ii. *the fact that research data collected for Market and Social Research is routinely de-identified (if this applies); and*
iii. *how long (if at all) any identifiable research information provided is likely to remain identifiable; and*
iv. *if applicable, the fact that, having participated in a Market and Social Research exercise, their contact details will be retained and that there is a reasonable likelihood that the individual will be re-contacted for Market and Social Research purposes (if this applies), except where the Research Organisation and client have reasonable grounds to decide that there are* ***genuine research concerns****; and*
v. *the fact that the Research Organisation wishes to disclose identifiable research information to a client organisation (if this applies). In these circumstances, the individual's explicit consent should be obtained to give practical effect to APP 6.1(a).*

In relation to matter (e)*, there will generally be no need to explain 'the main consequences (if any) for the individual if all or some of the information is not collected' since there will be no consequences for them – collection for research under this Code is always voluntary, and respondents should never be under the misapprehension that they are required to participate.*

In relation to matter (g)*, while the obligation is for Research Organisations to explain that their research information privacy policy contains information about their process for dealing with requests for access and correction, there is nothing to stop them from also simply explaining this along with the other matters when collecting identifiable research information. Research Organisations should explain that, while the information remains identifiable, the individual is allowed to, at his or her discretion, access that information, and seek to have part or all of that information corrected. If Research Organisations choose to offer individuals the option of having identifiable research information destroyed or de-identified, even though this is not an obligation under APP 13 (see below), then this option should also be explained in the notice given at the time of collection. Explanation of 'how' an individual can seek access, correction, etc., overlaps with the obligation to give contact details for the Research Organisation – organisations may choose to use the same or different contact details, provided they are clearly communicated.*

In relation to matter (h)*, while the obligation is for Research Organisations to explain that their research information privacy policy contains information about their process for handling complaints about a breach of this Code, there is nothing to stop them from also simply explaining this along with the other matters when collecting identifiable research information.*

In relation to matters (i) and (j)*, if disclosure is to be made to a client overseas (with the individual's consent – see (v) under matters (d)(e) & (f) above) – or to any other party overseas (e.g. for data processing) then the individual must be informed of this fact and, if practicable, the relevant country(ies) involved.*

Additional requirement: matters of which respondents should be made aware – sources of information and identity of client

5.3 Research Organisations must disclose the source of the research sample (e.g. customer information, information collected by researchers, publicly available lists such as a telephone directory or electoral roll, random digit dialling, door knocking) no later than the end of the collection of information, except where the Research Organisation and client have reasonable grounds to decide that there are genuine research concerns or where there is another compelling reason not to do so (e.g. it may expose one of the parties to legal action).

Explanatory Note:
Under the APPs, disclosure of sources may be required under APP 5.2(b) but is only an express obligation in relation to direct marketing (APP 7.6(e)). It is however best practice in data protection generally as well as having been an obligation on Research Organisations under the pre-2014 Code (MSRPP 1.5(j)). That obligation has been carried over into this Code. Provision is made for exceptions.

5.4 Research Organisations must disclose the identity of the client, unprompted, no later than the end of the collection of information, except where the Research Organisation and client have reasonable grounds to decide that there are genuine research concerns or where there is another compelling reason not to do so (e.g. it may expose one of the parties to legal action).

Explanatory Note:
Disclosure of client identity is not an obligation under the Act but is considered best practice. Non-disclosure should be an exception, only for compelling reasons, and the effect of non-disclosure must not be misleading or deceptive. The Research Organisation must always accurately describe how (and to whom) personally identifying research results may be disclosed to any entity other than the Research Organisation. The Research Organisation must always accurately disclose the identity and contact details of the Research Organisation.

Dealing with personal information

Australian Privacy Principle 6: Use or disclosure of personal information (as customised for the purposes of this Code)

Use or disclosure

6.1 If a Research Organisation holds identifiable research information about an individual that was collected for a particular purpose (the primary purpose), the Organisation must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or court/tribunal order;

(c) it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure; and the Research Organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

(d) the Research Organisation (the organisation) has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in; and the organisation reasonably believes that the collection, use or disclosure is necessary in order for the organisation to take appropriate action in relation to the matter.

(e) the Research Organisation reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf, of an enforcement body.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 Not applicable other than the exceptions now in 6.1(b)–(e).

Explanatory Note:
Although a range of secondary uses is permitted under APP 6, this Code provides that, in the conduct of market and social research, a Research Organisation must not use or disclose identifiable research information for any purpose other than a research purpose, except with the consent of the individual or if required by law. A research purpose may be the primary purpose for which the information was collected or a related secondary research purpose within the reasonable expectation of the individual and related to the primary purpose (directly related if sensitive information is involved).

Additional requirement: research use and disclosure

Re-use of identifiable research information for subsequent research

6.2A A Research Organisation may use identifiable research information for a research purpose provided that:

i. if re-contact of an individual who initially declined to participate is involved, the Research Organisation and client have genuine research concerns that warrant such re-contact; and

ii. if re-contact of an individual who has participated in a research exercise is involved:

a. the individual was informed of this likelihood at the time the information was collected, except where the research and client organisations have reasonable grounds to decide that there are genuine research concerns that justify not so notifying; or

b. any individual who, at the time of collection, indicated a wish not to be re-contacted for research purposes is excluded unless the research and client organisations have reasonable grounds to decide that there are genuine research concerns that warrant the individual's inclusion.

Disclosure of personal information for research

6.2B A Research Organisation may disclose identifiable research information provided that:

i. the disclosure is necessary for a research purpose; and

ii. only that part of the information considered necessary for this research purpose is disclosed; and

iii. if this research purpose could be achieved using de-identified information, the information is de-identified before being disclosed [APP 6.4]; and

iv. where the recipient is the client, the consent of all individuals who could be identifiable has been obtained, except where the personal information being disclosed to the client concerns individuals' research status. In this case:

a. the Research Organisation should take reasonable steps to ensure that the information concerning individuals' research status cannot be linked to individuals' research data about those individuals; and

b. the Research Organisation should obtain the client's agreement to restrict use of the information concerning individuals' research status only for the specific purpose of regulating the frequency of contacts of individuals in the client's subsequent research.

6.3 Not applicable (agencies only)

6.4 If subsection 16B(2) applies in relation to the collection of the identifiable research information by the Research Organisation (the organisation), it must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the organisation discloses it in accordance with subclause 6.1 or 6.2:

Explanatory Note:
Section 16B(2) of the Privacy Act sets out "permitted health situations" in relation to use and disclosure. These "permitted health situations" provide a narrower set of exceptions that are unlikely to arise in the context of Market and Social Research.

Written note of use or disclosure

6.5 If a Research Organisation uses or discloses identifiable research information in accordance with paragraph 6.1(e), the organisation must make a written note of the use of disclosure.

Related bodies corporate

6.6 If a Research Organisation is a body corporate and it collects identifiable research information from a related body corporate then this principle applies as if the Research Organisation's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by a Research Organisation of:

(a) identifiable research information for the purpose of direct marketing; or

(b) government-related identifiers.

Explanatory Note:
Research organisations subject to this Code do not use or disclose identifiable research information for direct marketing (see under APP7 below) but may handle government-related identifiers, in which case APP 9 will apply.

Australian Privacy Principle 7: Direct marketing (as customised for the purposes of this Code)

7.1 If a Research Organisation holds identifiable research information about an individual, the Research Organisation must not use or disclose the information for the purpose of direct marketing.

7.2 - 7.8 Not applicable.

Explanatory Note:
This principle applies to Research Organisations without any exceptions. Market and Social Research as defined in this Code does not allow for the use or disclosure of identifiable research information for direct marketing.
Furthermore, a prerequisite for eligibility for membership of AMSRO is the requirement that, unless in the furtherance and promotion of its own services (i.e. not in the actual conduct of Market and Social Research), a Research Organisation cannot engage in direct marketing or any other activity where the names and addresses of the people contacted (in the conduct of research) are to be used for individual selling, promotional, fund-raising or similar activities.

Australian Privacy Principle 8: Cross-border disclosure of personal information (as customised for the purposes of this Code)

8.1 Before a Research Organisation discloses identifiable research information about an individual to a person (the *overseas recipient*):

(a) who is not in Australia or an external Territory; and

(b) who is not the Research Organisation itself or the individual;

the Research Organisation must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of identifiable research information about an individual by a Research Organisation to the overseas recipient if:

(a) the Research Organisation reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the Research Organisation expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the Research Organisation.

Exceptions (e) and (f) are not applicable (agencies only)

Note: For ***permitted general situation***, see section 16A.

Explanatory Note:
The exceptions in APP 8.2 are unlikely to be relevant to handling of identifiable research information by Research Organisations.
A disclosure regulated by APP 8.1 may occur where a Research Organisation uses an affiliate or unrelated service provider outside Australia (such as a cloud service provider providing a cloud platform that is not confined to Australia) to analyse or otherwise handle identifiable research information on behalf of the Research Organisation, in circumstances where the identifiable research information is not fully encrypted and unable to be read by the offshore service provider or the handling of the identifiable research information does not remain fully under the control and direction of the Research Organisation.[13]
Whenever APP 8.1 applies, good practice is to ensure that an offshore service provider is fully aware of the requirements of the Australian Privacy Principles and provides contractual commitments to the Research Organisation to comply with the Australian Privacy Principles in the offshore service provider's handling of identifiable research information on behalf of the Research Organisation, including by ensuring that the identifiable research information is not further disclosed or used for any other purpose.
Note that where there are overseas disclosures of identifiable research information, that information remains governed by the APPs and the (Australian) Privacy Act, but may also become subject to data protection laws of other jurisdictions, including the General Data Protection Regulation of the European Union. Research Organisations should inform themselves of data privacy laws and other legal and regulatory requirements of any offshore jurisdiction in which identifiable research information may be held in any form that is not highly secure and able to be read only by the Research Organisation.

Australian Privacy Principle 9: Adoption, use or disclosure of government-related identifiers (as customised for the purposes of this Code)

Adoption of government-related identifiers

9.1 A Research Organisation must not adopt a government-related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government-related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation; see section 7A.

Use or disclosure of government-related identifiers

9.2 A Research Organisation must not use or disclose a government-related identifier of an individual unless:

[13] See para [8.7]-[8.15] of Chapter 8: APP 8 – Cross-border disclosure of personal information, rev July 2019, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation; see section 7A.

Note 2: For ***permitted general situation***, see section 16A.

Explanatory Note:
There may be circumstances in which a Research Organisation is contracted to undertake research that involves the collection and use of a government-related identifier. In such circumstances, the Research Organisation would have to satisfy itself that the use of the identifier was permissible under one of the exceptions in APP 9.2.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by a Research Organisation of a government-related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the Research Organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed; see subsections 100(2) and (3).

Explanatory Note:
It is not expected that any Research Organisations will be affected by regulations made under this provision.

Integrity of personal information

Australian Privacy Principle 10: Quality of personal information (as customised for the purposes of this Code)

10.1 A Research Organisation must take such steps (if any) as are reasonable in the circumstances to ensure that the identifiable research information that the Research Organisation collects is accurate, up to date and complete.

10.2 A Research Organisation must take such steps (if any) as are reasonable in the circumstances to ensure that the identifiable research information that the Research Organisation uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Explanatory Note:
In the context of Market and Social Research, the concept of quality of information has to be qualified, as responses given by respondents to surveys (research data) will usually be subjective and may not be objectively 'correct'.
While it is reasonable to expect Research Organisations to seek to ensure the quality of 'contact details' and 'research status' (the other two types of identifiable research information), the quality obligation in relation to 'research data' will be limited to ensuring that responses are accurately recorded and complete at the time of collection.
In the research context, research data is recorded at a point in time (e.g. the interview or completion of a questionnaire), and it would not be appropriate to change or update the data, even if the respondent later felt that the data did not represent their current views – see below re correction rights.
If a Research Organisation retains identifiable research information, when using or disclosing that information, it should:

a) where it concerns research data, warrant that the information is an accurate and complete record of the information supplied at the time of collection; and
b) where it concerns identifiable research information other than research data (i.e. contact details or research status), take reasonable steps to ensure that the information remains accurate, up to date, complete and relevant.

Once information has been de-identified, any obligation of a Research Organisation to update the information ceases.

Australian Privacy Principle 11: Security of personal information (as customised for the purposes of this Code)

11.1 If a Research Organisation holds identifiable research information, the Research Organisation must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) a Research Organisation holds identifiable research information about an individual; and

(b) the Research Organisation no longer needs the information for any purpose for which the information may be used or disclosed by the Research Organisation under this Code; and

(c) the information is not contained in a Commonwealth record; and

(d) the Research Organisation is not required by or under an Australian law, or a court/tribunal order, to retain the information;

(e) the Research Organisation must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Explanatory Note:
A Research Organisation must take reasonable steps to protect security of identifiable research information handled by that Research Organisation. Threats to personal information can be internal or external as well as malicious or unintentional. Privacy breaches can arise as a result of human activity or events such as natural disasters. Organisations should assume that human error will occur and design to mitigate risk and impact of human error.
Research Organisations should also take reasonable steps to mitigate risk and impact of malicious attacks that may lead to data breaches.
See further: OAIC, Guide to securing personal information, June 2018, available at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/; OAIC, Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), rev July 2019, available at https://www.oaic.gov.au/assets/privacy/guidance-and-advice/data-breach-preparation-and-response.pdf.

Additional Requirement: retention and disposal

11.3 A Research Organisation must retain identifiable research information only while the details of the identity of the individual whom the information is about continue to be necessary to be retained for research purposes. The information must be destroyed or de-identified once these purposes have been achieved. Where identifiable research information has been returned to a third party (in accordance with APP 6), any copies, including archived copies, must be destroyed or de-identified.

If a Research Organisation wishes to de-identify identifiable research information that exists in a physical form that makes de-identification impracticable (e.g. on paper), the information must be moved to another medium, de-identified, and the physical records then destroyed.

Where it is necessary to retain identifiable research information, identifying (contact) details must, if practicable, be stored separately from other information (research status and research data), with measures in place (e.g. by the use of an encrypted

intervening variable) to ensure the identity of the individuals cannot be readily revealed from the other information.

A Research Organisation must take reasonable steps to ensure that any identifiable research information that it discloses:

a. will be retained, used or disclosed by the recipient of the information only in a manner that is consistent with this Code; and

b. will be protected by the recipient from misuse, interference and loss and from unauthorised access, modification, use and disclosure; and

c. will be used or disclosed by the recipient only for a specified limited purpose and will be destroyed or de-identified once this purpose has been achieved. Where identifiable research information has been returned by the recipient to a third party (in accordance with APP 6) any copies, including archived copies, must be destroyed or de-identified.

A Research Organisation may disclose de-identified information freely, provided that there is no reasonable likelihood that the disclosed information could be used to identify one or more of the individuals who participated in the research, such as where the pattern of answers could reveal their identity.

Access to, and correction of, personal information

Australian Privacy Principle 12: Access to personal information (as customised for the purposes of this Code)

Access

12.1 If a Research Organisation holds identifiable research information about an individual, the Research Organisation must, on request by the individual, give the individual access to the information.

12.2 Not applicable (agencies only)

Exception to access

12.3 Despite subclause 12.1, the Research Organisation is not required to give the individual access to the identifiable research information to the extent that:

(a) the Research Organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the Research Organisation and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the Research Organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the Research Organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Research Organisation's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the Research Organisation in connection with a commercially sensitive decision-making process.

Explanatory Note:
It is unlikely that a Research Organisation would need to take advantage of any of these exceptions to deny access but the exceptions are available. For the purposes of exception (c), 'frivolous or vexatious' includes:

- *repeated requests for access to personal information that has already been provided to the requester*
- *a request that contains offensive or abusive language, or that does not appear to be a genuine request for personal information*
- *a repeat request for personal information that an organisation has earlier explained to an individual it does not hold, has been destroyed, or cannot be located after a reasonable search*
- *a request made for the apparent purpose of harassing or intimidating the staff of an organisation or interfering unreasonably with its operations.*

Dealing with requests for access

12.4 The Research Organisation must:

(a) respond to the request for access to the identifiable research information within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the Research Organisation refuses:

(a) to give access to the personal information because of subclause 12.3; or

(b) to give access in the manner requested by the individual;

then the Research Organisation must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the Research Organisation and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 Not applicable (agencies only).

12.8 If the Research Organisation charges the individual for giving access to the identifiable research information, the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the Research Organisation refuses to give access to the identifiable research information because of subclause 12.3, or to give access in the manner requested by the individual, the Research Organisation must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the Research Organisation refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Australian Privacy Principle 13: Correction of personal information (as customised for the purposes of this Code)

Correction

13.1 If:

(a) a Research Organisation holds identifiable research information about an individual; and

(b) either:

(i) the Research Organisation is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

then the Research Organisation must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the Research Organisation corrects personal information about an individual that the Research Organisation previously disclosed to another APP entity; and

(b) the individual requests the Research Organisation to notify the other APP entity of the correction;

then the Research Organisation must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the Research Organisation refuses to correct the identifiable research information as requested by the individual, the Research Organisation must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the Research Organisation refuses to correct the identifiable research information as requested by the individual; and

(b) the individual requests the Research Organisation to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

then the Research Organisation must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the Research Organisation:

(a) must respond to the request within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

Explanatory Note:
A request may be made in a variety of ways and need not be made in whatever way a Research Organisation would prefer to receive such requests, or nominates as the only way in which that Research Organisation will accept such requests.
If a Research Organisation receives a request from an individual to correct his or her identifiable research information, the Research Organisation's response should depend on the type of information:
Where the request concerns research data, the Research Organisation should:

i. explain to the individual that 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; but also
ii. at the request of the individual, associate with the information a statement that the information is (in the individual's opinion) inaccurate, out of date, incomplete, irrelevant or misleading.

Because of the importance of maintaining the integrity of research, Research Organisations will generally decline to correct research data (survey responses), offering only the option of an associated statement where practicable, and information about the right to complain to the OAIC or recognised External Dispute Resolution (EDR) scheme where applicable. (No such EDR schemes are available at the commencement of this Code.) In limited cases, it will be impracticable to associate a statement because of the way the research data is held.
Where the request concerns identifiable research information other than research data (i.e. contact details or research status), the Research Organisation should either:

i. correct the information so that it is accurate, up to date, complete, relevant and not misleading; or

ii. where a record of the uncorrected information is required for research purposes, associate with the information a statement that the information is (in the individual's opinion) inaccurate, out of date, incomplete, irrelevant or misleading.

Additional requirement: destruction or de-identification on request

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

i. the request is frivolous or vexatious; or

ii. destruction, deletion or de-identification would have an unreasonable impact upon the privacy of other individuals; or

iii. the Research Organisation reasonably believes that destroying, deleting or de-identifying the information would pose a serious threat to the life, health or safety of any individual or to public health or public safety; or

iv. destroying, deleting or de-identifying the information would reveal the intentions of the Research Organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

v. destroying, deleting or de-identifying the information would be unlawful; or

vi. retaining the identifiable information is required or authorised by or under an Australian law or a court/tribunal order; or

vii. the Research Organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in; and destroying, deleting or de-identifying the information would be likely to prejudice the taking of appropriate action in relation to the matter; or

viii. destroying, deleting or de-identifying the information would be likely to prejudice one or more enforcement-related activities conducted by or on behalf of an enforcement body; or

ix. where the Research Organisation is contractually obliged to retain the identifiable research information.

Explanatory Note:
This Code provides an additional right for research subjects to request destruction or de-identification over and above the right to correction in APP 13. This continues the same right that existed under the predecessor Code (MSRPP 6). The right is subject to similar exceptions to those that apply to requests for correction.

In many cases, research data will not be corrected because of the purpose for which the information is held and it is unlikely that a Research Organisation would need to take advantage of any of these exceptions to deny a request for destruction, etc., (except under (ix), which is more common).

For the purposes of exception (i) above, 'frivolous or vexatious' includes:

- *repeated requests for correction of personal information that has already been corrected;*
- *a request that contains offensive or abusive language, or that does not appear to be a genuine request for personal information;*
- *a repeat request for correction of personal information that an organisation has earlier explained to an individual it does not hold, has been destroyed, or cannot be located after a reasonable search; and/or*
- *a request made for the apparent purpose of harassing or intimidating the staff of an organisation or interfering unreasonably with its operations.*

(These examples are taken from the OAIC APP Guidelines.)

In respect of exception (ii) above, destruction or de-identification as requested may involve the destruction or de-identification of information relating to other individuals; in this case, there would potentially be an 'unreasonable impact upon the privacy of those other individuals and the request need not be complied with, For example, honouring a request for destruction could result in information about another person being incomplete.

In respect of exception (v) above, there may be some circumstances, particularly when working for government clients, where Research Organisations are required to keep data for a specific period for re-analysis and destruction may be unlawful, although de-identification should always be considered.

For the purposes of exception (viii) above, 'enforcement-related activities' has the same meaning as in the Privacy Act s.6.

F. GOVERNANCE

Code Administrator

a. The Code Administrator for this Code is AMSRO. In practice, this Code is administered by the AMSRO Secretariat, under the direction of the AMSRO Board.

b. AMSRO will fund the administration of this Code in such manner as the AMSRO Board considers appropriate, having regard to the resource requirements necessary for the effective execution of those tasks described in subclause F(c).

Tasks of the Code Administrator

c. In administering this Code, the AMSRO Secretariat will perform the following tasks:

i. maintain an accurate and up-to-date online list of AMSRO members, which doubles as a public register of Research Organisations that are bound by this Code;

ii. commission periodic reviews of this Code in accordance with Part G;

iii. produce a written response to a report resulting from an independent Code review;

iv. consider the need for any variation of this Code, and make any consequent applications;

v. monitor and report on compliance with this Code (see Part H);

vi. make available on the AMSRO website the following:

(a) information about this Code;
(b) a copy of the most current version of this Code;
(c) contact details for the Code Administrator;
(d) information about making complaints in relation to matters contained in this Code;
(e) the annual report on the operation of this Code required under Part H;
(f) a link to the website of the Commissioner;
(g) any other information that the Code Administrator considers relevant to the efficient functioning of this Code.

vii. perform such other tasks as the AMSRO Board considers necessary or desirable for the effective operation of this Code, including but not limited to the establishment and management of a formal complaints-handling process relating to alleged breaches of this Code.

viii. In relation to tasks a.ii-v, the Administrator will be assisted and advised by AMSRO's Privacy Compliance Committee.

d. AMSRO has established a Privacy Compliance Committee, comprising an independent chair, at least two industry representatives and one consumer representative, which meets at least twice a year.

e. The Privacy Compliance Committee terms of reference include the following functions relevant to this Code:

"To make recommendations on matters including, but not limited to:

1) The Code Reviewer's recommendations concerning streamlining industry Guidelines to clarify how they work in conjunction with the Code;

2) The Code Reviewer's recommendations concerning implementing an explicit privacy component into industry quality audits;

…

5) Industry awareness/education regarding privacy issues, including information sheets, FAQs and best practice;

…

7) Systemic issues arising from privacy complaints."

f. The Privacy Compliance Committee will advise the Code Administrator about the timing and conduct of the periodic independent review of this Code under Part G.

g. The Privacy Compliance Committee may be required by the Code Administrator to participate in any formal complaints-handling process that might be established by the Code Administrator relating to addressing alleged breaches of this Code.

G. REVIEW

Independent Code Review

a. This Code is subject to periodic independent review by a reviewer to be appointed by the AMSRO Board for each review.

b. The purpose of Code reviews is to ensure that this Code is meeting its objectives and remains effective and relevant.

c. There will be a review of this Code at least every five years, but the Code Administrator may commission a review at any time; for example, if regular monitoring indicates a lack of compliance with this code or if the Code Administrator becomes aware of systemic issues that would justify a review.

d. The terms of reference for each review will be drawn up by the Code Administrator in consultation with the Privacy Compliance Committee.

e. Each review will be funded by AMSRO in such manner as the AMSRO Board considers appropriate, having regard to the resource requirements necessary for the effective execution of the review.

f. Reports of the independent code review will include recommendations for any amendments to this Code that are considered necessary or desirable for the effective operation of this Code.

Consultation

g. In conducting an independent review, the Code Administrator will notify the Commissioner of the review, and the Independent Code Reviewer will seek the views of the Commissioner, government agencies, industry representatives, consumer

representatives, the general public and other persons or bodies as appropriate in Australia and internationally regarding the operation of this Code and in relation to suitable revisions and amendments.

Reporting following an Independent Code Review

h. The report of the Independent Code Reviewer shall be made publicly available online and shall outline the issues raised by the review and the findings of the review.

i. The report shall be accompanied by a response from the Code Administrator, outlining the actions taken, or that will be taken, by the Code Administrator and/or the Research Organisations bound by this Code to address issues identified by the review.

Variation of the Code

j. Following a recommendation of an Independent Code Review, or for any other reason, the Code Administrator may apply to the Commissioner for variation of the Code.

k. Any such application would follow the process set out in the Act and guidance issued by the Commissioner.

H. MONITORING AND REPORTING

a. Research Organisations must report annually, by 31 August, to the Code Administrator, on the number, nature and outcomes of any complaints received about Breaches of this Code.

Explanatory Note:
AMSRO, as the Code Administrator, will issue instructions for the reporting of complaints, including the method of reporting, which is likely to involve a simple completion of an online form. This reporting requirement will have implications for the records that a Research Organisation will need to keep during a year (see Explanatory Note to APP 1.2).

b. Research Organisations must report systemic issues in relation to their compliance with this Code, or serious and repeated Breaches of this Code, to the Commissioner as soon as they become aware of them.

c. 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 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 the handling of identifiable research information that might reasonably be expected to be mitigated by appropriate action taken by Research Organisations generally.

d. Research Organisations must handle inquiries and complaints received from individuals as to the handling of identifiable research information about those individuals courteously, promptly and efficiently. Research Organisations should establish reliable processes and procedures for handling inquiries and complaints received from individuals as to the

handling of identifiable research information, including by taking reasonable steps to address special needs and requirements of individuals with disabilities or particular vulnerabilities. In general, responses should be provided within 30 days.[14]

e. The Code Administrator will monitor compliance by Research Organisations with this Code and will investigate serious and repeated breaches and systemic issues about code compliance.

f. The Code Administrator will publish an Annual Report on the operation of this Code and make it available both to the Commissioner and publicly, including online. 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 review, including complaints or other concerns of any individual raised with a Research Organisation in relation to or within the scope of operation of this Code during the year in review, and consider any responses of Research Organisations in relation to such matters, before finalising and publishing an Annual Report on the operation of this Code. The Annual Report will include a summary of complaints handled by Research Organisations and reported to the Code Administrator under clause H(a).

g. The Code Administrator will report systemic issues or serious and repeated breaches of this Code to the Commissioner as soon as it becomes aware of them.

Improper conduct

h. If a Research Organisation subject to this Code acts in a manner that, in the AMSRO Board's opinion, constitutes seriously improper conduct in relation to this Code, the AMSRO Board shall direct the Code Administrator to notify the Research Organisation of the conduct.

i. Within 7 business days of receipt of notification by the Code Administrator of an opinion by the AMSRO Board concerning seriously improper conduct by the Research Organisation, the Research Organisation must:

   i. take all reasonable steps to rectify the seriously improper conduct; and

   ii. notify the Code Administrator of the steps taken to rectify the seriously improper conduct.

j. If the Research Organisation fails to comply adequately with clause g. above then the AMSRO Board will issue a final notice requiring the Research Organisation to rectify the seriously improper conduct within 7 business days.

k. Where the AMSRO Board is satisfied that seriously improper conduct has occurred in relation to this Code, AMSRO may take such remedial action against the Research Organisation as is permitted under its Rules of Association and/or terms of membership, as varied from time to time, including suspension or expulsion.

These misconduct provisions operate independently of the complaint provisions of the Privacy Act and the enforcement role of the Commissioner.

[14] See further: OAIC, Handling privacy complaints, October 2016, available at https://www.oaic.gov.au/privacy/guidance-and-advice/handling-privacy-complaints/