

GUIDELINES FOR THE CONTRACTING OUT OF RESEARCH ACTIVITIES

Part 1: Introduction

The need for a document of this kind arises mainly from the fact that, while the Market & Social Research Privacy Principles (M&SRPPs) in the Privacy Code regulate the conduct of research organisations that subscribe to these principles, they do not necessarily regulate the conduct of contractors to those research organisations. In cases where contractors are bound by the National Privacy Principles (NPPs) (or any other set of privacy principles), which are less strict than the M&SRPPs in some respects, research organisations need to ensure that their contracting of activities does not lead to a breach of their responsibilities in relation to the M&SRPPs.

The guidelines that follow can be used by research organisations, should they outsource activities to contractors that are not bound by the M&SRPPs. These would only be required in situations where fulfilling the contractual agreement requires the contractor to handle identified information on the research organisation's behalf.

While AMSRS and AMSRO have taken reasonable care in the preparation of this document, it is meant only as a guide and organisations should not rely upon this document in the preparation of any contract or other document. Legal advice should be sought about specific issues relating to privacy for individual contracts.

1.1 Who is responsible?

Where a research organisation has failed to exercise control where it should have, then it would still be subject to the requirements of the M&SRPPs in relation to that information and the individual may be able to assert his/her rights under the Privacy Act against the research organisation.

In situations where a research organisation is not in any way responsible for an interference with the privacy of an individual by a contractor, it is desirable that the contractor be made responsible for this interference as a breach of its privacy obligations under its contract with the research organisation.

1.2 Creating privacy protection through contractual terms

It is of great importance that, in any outsourcing agreement, the rights of the individual under the Privacy Act are preserved as far as possible and the research meets its security obligations under M&SRPP 5. The underlying premise of this

Note: Action should not be taken solely on the information given in this document. Legal or professional advice should be sought to ensure no misinterpretation occurs. Please take the time to read the important disclaimer.

document is that research organisations are ultimately accountable for the way in which identified information given to contractors is handled.

M&SRPP 5 requires research organisations to protect identified information that it holds against misuse by reasonable security safeguards, including doing everything within their power to ensure that service providers handling the information do not misuse it or transfer it without authority.

One method of achieving compliance with M&SRPP 5 is by the inclusion of appropriate provisions in outsourcing contracts. This document provides guidelines, both to cover the security obligation and to extend, as far as possible, the protection of the other M&SRPPs.

1.3 Guidelines

What follows in Parts 2, 3 and 4 is a set of guidelines and advice applicable to contracts for outsourced research functions involving identified information.

For those research organisations seeking the assistance of private law firms (which we strongly recommend), it is suggested that this document be brought to their attention.

Part 2 outlines guidelines relevant to common outsourcing contracts and provides commentary on those guidelines, where appropriate. Incorporation of these guidelines in any contract involving identified information, or otherwise, should ensure that the obligations of a research organisation under the M&SRPPs are passed to a contractor.

Part 3 outlines general considerations for research organisations relevant to most outsourcing contracts. For example, additional requirements may be necessary where a research organisation wants to approve of all persons who will have access to identified information.

Part 4 sets out guidelines that may be incorporated in special circumstances. They may not be relevant in many outsourcing situations, for example, where the contractor had only transient possession of identified information and obtained the information relevant to the contract directly from the research organisation.

However, where the contractor is maintaining a database on behalf of a research organisation over a protracted period, it is important to make reasonable endeavour to ensure that individuals have rights in relation to access to, amending or appending of, and destruction, deletion and de-identification of, the information, as if the database were in the possession of the research organisation.

If a contractor collects identified information on behalf of a research organisation, the process of collection should accord with the principles in M&SRPP 1 and the contract should incorporate objectives to that effect.

Part 2: Guidelines relevant to most contracts

2.1 Definition of “identified information”

For the purposes of an agreement, “identified information” could be defined to mean information or an opinion, whether true or not, and whether recorded in a material form or not, provided by, or held in relation to, an individual whose identity is apparent, or can reasonably be ascertained.

This is the definition given to “identified information” in the M&SRPPs.

2.2 Security

The contractor should take all reasonable measures to ensure that identified information held in connection with, or in relation to, this agreement is protected from misuse and loss and from unauthorised access, modification, disclosure and transfer in accordance with the security procedures set out in Schedule [].

The contractor should not vary the security procedures set out in Schedule [] without the prior written approval of the research organisation.

A schedule should be attached setting out security procedures approved by the research organisation. The nature and extent of these will naturally vary depending on the circumstances of the contract. For example, more stringent controls might be appropriate where sensitive information is involved.

2.3 Use

The contractor should be prohibited from using any information held in connection with, or in relation to, the agreement in any way other than for the purposes of fulfilling its obligations under this agreement, unless it has the written authority of the research organisation to do so.

Research organisations should take care to see that any obligations that the contractor has under the agreement do not go beyond a “use” that the research organisation itself would be permitted under M&SRPP 2.

2.4 Disclosure and transfer

The contractor is prohibited from disclosing and/or transferring any information held in connection with, or in relation to, the agreement in any way other than for the purposes of fulfilling its obligations under this agreement, without the written authority of the research organisation. The contractor should be required immediately to notify the research organisation in writing where it becomes aware that a disclosure and/or transfer of identified information might be required by law.

While acknowledging that the contractor may have a legal duty to transfer identified information, it should let the research organisation know as soon as possible so that the research organisation may consider its position in relation to the legality of the requested transfer and have the opportunity to intervene in any proceedings before any transfer is made.

2.5 Disclosure and transfer of identified information outside Australia

The contractor is prohibited from disclosing and/or transferring any identified information held in connection with, or in relation to, this agreement outside Australia, or allowing parties outside Australia to have access to it, without the prior approval of the research organisation.

While this form of disclosure or transfer would be covered by 2.4, there may be value in stating this prohibition specifically because of the high risk associated with trans-border flows of information. Generally, once information goes beyond Australia's borders, it may be either impractical or impossible for a research organisation to prevent any unauthorised use, disclosure or transfer of that information.

2.6 Employee awareness of privacy requirements and undertakings

The contractor should ensure that any employee of the contractor or any contractor requiring access to any identified information held in connection with this agreement executes an undertaking in writing to not access, use, disclose, transfer or retain identified information except in performing their duties of employment and is informed that failure to comply with this undertaking may be a criminal offence and may also lead the contractor to take disciplinary action against the employee.

For reasons of enforceability, it is suggested that the employee undertaking referred to be a deed, which should be attached to the contract.

This employee undertaking may not be sufficient to make employees fully aware of their responsibilities.

2.7 Advising the research organisation of any breach of the privacy guidelines

The contractor should, in respect of any identified information held in connection with, or in relation to, this agreement, immediately notify the research organisation where the contractor becomes aware of a breach of guidelines [2.2, 2.3, 2.4, 2.5 and 2.6] by itself or any sub-contractor.

The contractor should be obliged to immediately notify the research organisation when it becomes aware that it has breached the contractual provisions relating to security, unauthorised use, disclosure or transfer of identified information.

2.8 Reasonable requests, directions and guidelines

The contractor should in respect of any identified information held in connection with, or in relation to, this agreement co-operate with any reasonable requests or directions of [the research organisation's delegate].

While a contractor's actions cannot be directly affected by recommendations or determinations of the Privacy Commissioner under the Privacy Act, this provision should ensure that the research organisation endeavours to ensure that the contractor does anything that the Privacy Commissioner may require the research organisation to do if the research organisation had not outsourced the particular function.

2.9 Handling of complaints

A complaint alleging an interference with the privacy of an individual in respect of any services performed under an agreement should be handled by the research organisation and in accordance with the following procedures:

- (i) *where the research organisation receives a complaint alleging an interference with the privacy of an individual by the contractor or any sub-contractor, it should immediately notify the contractor in writing of*

only those details of the complaint necessary to minimise any breach or prevent further breaches of the above guidelines;

- (ii) where the contractor receives a complaint alleging an interference with the privacy of an individual by the contractor or any sub-contractor, it should immediately notify the research organisation in writing of the nature of the complaint and should only release to the research organisation the identified information concerning the complainant; and*
- (iii) after the research organisation has given or been given or received written notice in accordance with (i) or (ii), it should take reasonable steps to keep the contractor informed of all progress with the complaint as it relates to the actions of the contractor in connection with the allegation of an interference with the privacy of an individual.*

2.10 Ensuring contractual clauses have effect after the contract has ended

Contractual clauses incorporating the guidelines should continue to have effect and should not merge after the termination or completion of the agreement.

Even though contracts will normally provide for all identified information to be returned at the end of the agreement or be destroyed (see 3.1), it is prudent to ensure that, should any identified information inadvertently remain with the contractor, the protection that existed during the agreement continues to operate after the agreement has ended. In addition, where a breach comes to light after the agreement has ended, the relevant contractual clauses should also continue to apply.

Part 3: General considerations

3.1 Ensuring data security at end of agreement

The research organisation should endeavour to ensure that the contract adequately deals with what is to happen to any identified information in the possession of the contractor on completion or termination of the contract. If data are to be destroyed or deleted by the contractor, adequate security measures and timeframes should be specified in the contract.

3.2 Auditing of compliance with security and privacy guidelines

Research organisations should include an appropriate clause to give the research organisation access to the contractor's premises, records, equipment and the like to ensure that the contractor and the employees of the contractor are complying with their obligations under the agreement as to security, use, disclosure and transfer of identified information.

3.3 Employee access to identified information

Research organisations may wish to consider whether they want input in determining which of the contractor's employees will have access to identified information. This will, of course, depend on the sensitivity of the identified information that is the subject of the agreement.

3.4 Sub-contracting

Most agreements will have clauses that prevent sub-contracting without the consent of the research organisation. If a research organisation considers it appropriate to give approval to the contractor to sub-contract all or part of those activities covered by the contract, before giving consent it should ensure that all guidelines relating to protection of identified information are included in any agreement between the contractor and a sub-contractor. The research organisation may also wish to become a party to the agreement to subcontract.

Should sub-contracting occur, the research organisation should satisfy itself that arrangements are in place to ensure that the undertakings referred to in 2.6 are signed by any of the sub-contractor's employees having access to identified information.

The agreement to subcontract should contain a provision whereby a contractor that becomes aware of a breach of any of the privacy protection guidelines by a sub-contractor must immediately notify the research organisation in writing of this breach (see 2.7).

Part 4: Guidelines relevant in special circumstances

In many contract arrangements, the contractor will only have short term possession of identified information provided by the research organisation for processing. Its functions under the contract will not include collection of identified information from third parties or medium or long-term storage of data. In these cases, the privacy guidelines suggested in Parts 2 and 3 of this paper would generally suffice.

Where the contractor, as well as processing data supplied by the research organisation, undertakes additional long-term research organisation functions such as data storage or collection, additional privacy guidelines will need to be incorporated into the research organisation's contractor agreement. The way in which the guidelines are incorporated will vary according to the extent to which the research organisation retains direct control over the activities of the contractor - where a high level of control is retained, relatively simple contract provisions binding the contractor to abide by the directions of the research organisation would probably be sufficient.

Where the contractor is allowed some discretion in determining identified information handling practices, it should be bound by the same standards in exercising that discretion as if it were a research organisation for the purposes of the Privacy Act. In the material set out below, alternative guidelines are suggested in some areas to cater for different contract arrangements, allowing varying levels of discretion to the contractor in the handling of identified information.

In deciding whether to contract out functions, and the extent to which contractors should be permitted to exercise discretion as to how those functions are carried out, research organisations should take account of the fact that these decisions have privacy implications. Allowing an outside body to exercise a measure of discretion in handling identified information obtained by the research organisation or on the research organisation's behalf may have an adverse affect on privacy and in some cases, may be so adverse as to lead a research organisation to decide against outsourcing that function.

4.1 Data quality

Normally, the contractor's obligation will be limited to ensuring that the data provided to it is accurately recorded and stored - it will be the research organisation's responsibility to review and amend the data to ensure accuracy. In this situation, the following clause might be considered:

The contractor should take all reasonable steps to ensure that identified information provided to it in connection with, or in relation to, this agreement is accurately recorded and is not amended except as directed by the research organisation.

4.2 Access, destruction, deletion, de-identification and correction

In most cases where contractors are responsible for the storage of a database, requests for access to, destruction, deletion or de-identification of or correction of identified information will be received and dealt with by the research organisation, which will obtain information from the contractor, and instruct the contractor to act as appropriate.

In this case, it is probably not necessary to include provisions relating to access, destruction, deletion, de-identification and correction into the contract, provided it is clear that the contract obliges the contractor to provide information held in connection with the arrangement to the research organisation on request, and to destroy, delete, de-identify or correct the information at the research organisation's direction. Research organisations would be expected to respond to requests for access, destruction, deletion, de-identification or correction of the information, as if it were held by them.

In cases where decisions on access, destruction, deletion, de-identification and correction are made by the research organisation, but requests from individuals may be directed in the first instance to the contractor, the following clause might be considered:

The contractor should, if it receives a request from an individual for access, destruction, deletion, de-identification or correction of identified information about the individual held by the contractor in connection with, or in relation to, this agreement, promptly [or within a set period] provide written notice to the research organisation of the request.

In cases where a contractor will have direct responsibility for responding to requests for access, destruction, deletion, de-identification and correction by individuals, the following guidelines are suggested. It is expected that such arrangements will be rare.

The contractor should undertake to the research organisation that it would:

- *permit individuals to access any identified information about themselves held by the contractor in connection with, or in relation to, this agreement; and*
- *permit individuals to have part or all of any identified information about themselves held by the contractor in connection with, or in relation to, this agreement deleted, destroyed or de-identified;*

except to the extent that the research organisation would be required or authorised to refuse to provide the individual with access, destruction, deletion or de-identification rights in relation to a record containing that information under the Market and Social Research Privacy Principles; and

- *having received a request from an individual to correct any identified information about themselves held by the contractor in connection with, or in relation to, this agreement, either correct its records or append the corrected information thereto.*

Since this clause refers to grounds for refusal of access, destruction, deletion and de-identification laid down in the M&SRPPs, the contractor would probably need to liaise with the research organisation about both procedures and individual requests.

4.3 Collection

In those cases in which contractors collect identified information on behalf of a research organisation, the nature of the information collected, and the method and manner of collection, should generally be specified by the research organisation. The following might be considered in relation to collection of identified information by the contractor:

The contractor should only collect identified information in connection with, or in relation to, this agreement as directed by the research organisation or specified in Schedule [] to this agreement, and should collect it in accordance with the procedures specified in Schedule [] to this agreement.

The procedures for collection of information should comply with the requirements of M&SRPP 1.