AMSRO
ASSOCIATION OF MARKET AND SOCIAL RESEARCH ORGANISATIONS

Mr Andrew Solomon
Assistant Commissioner
Dispute Resolution Branch
Office of the Australian Information Commissioner

Sent via email - consultation@oaic.gov.au

27 October 2017

Dear Mr Solomon,

RE: NOTIFIABLE DATA BREACHES SCHEME (NDB)

AMSRO RESPONSE TO THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER'S REQUEST FOR FEEDBACK ON DRAFT RESOURCES

Introduction

The Association of Market and Social Research Organisations (AMSRO) is the peak industry body representing over 70% of market and social research organisations in Australia. Handling the personal data of a very large number of Australian citizens requires AMSRO to invest significantly in the protection of personal privacy.

AMSRO is the only organisation which has an Industry APP Privacy Code approved by the Office of the Australian Information Commissioner (OAIC). AMSRO has a dedicated Privacy Compliance Committee, which meets on a regular basis and operates continuously to monitor privacy issues and provide proactive advice to our members.

The Privacy Compliance Committee has an independent chair and the members are drawn from privacy consumers and industry experts.

The following response to the OAIC's Draft Resources is provided by AMSRO's Privacy Compliance Committee. Firstly however, AMSRO would like to take this opportunity to commend the OAIC on its Draft NDB Resources and we look forward to encouraging their use by our members.

1. **Assessing a suspected data breach**

Organisations that suspect an eligible data breach may have occurred are required to undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm.

AMSRO considers that some areas of this Draft Resource may be enhanced by streamlining and clarifying the data breach response procedure. The initial assessment of most data breaches will be conducted in a crisis management situation and practitioners would benefit from having a clear and easily accessible procedure to follow.

AMSRO therefore suggests the Draft Resources would benefit with the inclusion of a flow chart or info-graph that provides a simplified step-by-step procedure (incorporating the OAIC's data response key points below):

1. **Initiate:** decide whether an assessment is necessary and identify which person or group will be responsible for completing it
2. **Investigate:** quickly gather relevant information about the suspected breach, including, for example, what personal information is affected, who may have had access to the information and the likely impacts, and
3. **Evaluate**: make a decision, based on the investigation, about whether the identified breach is an eligible data breach (see *Identifying eligible data breaches*).

Furthermore, assessing a data breach and identifying what constitutes a '*serious ('eligible') data breach'* remains a key concern for AMSRO as determining '*serious harm'* is still likely to cause some confusion.

> *'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Entities should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm.*

AMSRO recommends a series of high-level examples or case studies be provided to assist practitioners in this regard.

With regards to *Remedial Action*, it might be helpful to reiterate (to the potentially affected data subjects) the value of remedial action, that is:

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

2. What to include in an eligible data breach statement

For the most part, the Draft Resources do meet the needs but there remains an area of concern for AMSRO members regarding the responsibility of '*other parties involved in the data breach'* i.e. third-party disclosure and liability.

In particular, the situation of our members who handle personal data at the request of their clients.

Whilst AMSRO appreciates that the Privacy Act does not require this level of information, additional recommendations from the OAIC regarding a client's potential responsibility or liability for breach notification and remediation would be helpful.

AMSRO therefore welcomes further clarification as to who is ultimately responsible for notifying the individuals concerned and preparing a data breach statement for the Commissioner. (Again, some high-level suggestions could be provided as to the content of agreements or contracts which set out the responsibilities to protect personal data from breaches and to clearly establish which parties are actually responsible for the decision to notify breaches. This level of information may well avoid confusion and timing delays with respect to notifying affected individuals after a breach.)

3. Exceptions to notification obligations

As mentioned in an earlier submission, practitioners would benefit from a reminder that all organisations dealing with personal data, that the legislation is a minimum standard and organisations should aim to ensure that they strive for a higher level of personal data protection wherever possible. By way of example, AMSRO member organisations (large and small business) opt in to the strict industry practices underpinned by the Privacy Code. However not all organisations collecting personal information operate under these principles.

This is important for AMSRO members who may be working for clients who could in the future be reluctant to notify if there is some ambiguity about exemptions or for other reasons. This has not been an issue to date but may occur in the future.

4. The draft form to assist organisations in preparing a statement about an eligible data breach to the Australian Information Commissioner

The Draft Form captures the necessary requirements.

In summary, the Draft Resources could be enhanced by:

a) An abbreviated, easy-to-follow assessment guide or info-graph to ensure there is no confusion around identifying an '*eligible data breach likely to result in serious harm to any of the individuals to whom the information relates*'.
b) Greater emphasis on the value of having contractual obligations that clearly allocate responsibility to prevent and respond to data breaches; this is critical where responsibility is split between different parties such as the clients and their service providers and/or where some entities handling data are not covered by the Privacy Act.

c) A reminder that the practical purpose of the mandatory requirement to notify about a data breach is to put the data subject who might be affected, in a position where they can, as quickly as possible, make their own assessment of its potential seriousness in their individual case, understand what has happened, and make their own choices about what if anything to do as a remedy or mitigation, and how quickly to do it. While this may involve inconvenience, effort, or embarrassment for those dealing with the data breach, and the difficulty of working out the potential seriousness for those affected by an ambiguous or marginal breach, the possible adverse legal and reputation impacts of a delayed, incoherent or ineffective response arise from the potential for depriving the data subject of the best chance to sort out their own affairs before any serious impacts have actually manifest.

We trust you find our comments helpful. Should you require any further detail regarding the feedback provided please don't hesitate to contact us.

Kind regards,

Terry Aulich
Chair
AMSRO Privacy Compliance Committee
E: aulich@aulich.com.au

Sarah Campbell
Executive Director
AMSRO
E: sarah@amsro.com.au