AMSRO

ASSOCIATION OF MARKET AND SOCIAL RESEARCH ORGANISATIONS

Mr Timothy Pilgrim
Australian Information Commissioner
Office of the Australian Information Commissioner

Sent via email - consultation@oaic.gov.au

13 July 2017

Dear Mr Pilgrim,

RE: NOTIFIABLE DATA BREACHES SCHEME (NDB)

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

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 questions is provided as a result of AMSRO's participation in the OAIC's NDB scheme roundtable (held May 3), the Privacy Compliance Committee's considerations and those of the AMSRO Board. AMSRO welcomes the opportunity for Australian organisations to provide feedback, as it will help to add further value to the final OAIC advice. AMSRO would be happy to work with the OAIC further in the development of the guidelines if required.

Question 1: Are the Draft Resources clear, relevant and practical?

The draft resources cover most areas where organisations are likely to encounter difficulties. AMSRO considers that some areas of special interest to our industry may need some further elaboration. In particular, the situation of our members who handle personal data at the request of their clients is not covered in terms of a client's potential responsibility for breach notification and remediation.

Question 2: Do the Draft Resources meet the needs of agencies and organisations in understanding the new requirements under the NDB scheme?

For the most part the Draft Resources do meet the needs but there will be obvious difficulties encountered where exemptions are discussed since there are already exemptions under the Privacy Act, which allow some small businesses to have a lower requirement for privacy protection. Similarly, the specific exemptions for notification of data breaches is a possible area where confusion could exist.

AMSRO suggests that the OAIC, in any further papers on this subject, remind 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.

Question 3: Are there any topics that you believe the Draft Resources should cover that have not been covered or should have been covered in greater detail?

In the Draft Resources, 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 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.

The Draft Resources could also emphasise more the need for those who handle personal information to have clearly established and documented procedures for preventing and dealing with data breaches. Many data breaches are dealt with in a crisis management situation and established procedures should help to provide a clear passage through the difficulties. Such established procedures also provide an audit trail and learning opportunity for organisations faced with a breach. AMSRO would suggest that the OAIC should stress that the procedures for data breach notifications should strongly advise senior management to sign off those procedures and that privacy protection and mitigation be a senior management responsibility.

Question 4: Are there any practical examples you could share to help illustrate the operation of the NDB scheme?

AMSRO's members, by virtue of their need to maintain public trust in social and market research organisations, are already intimately involved in the protection of personal data and most of the industry processes depend on standard practices of de-identification, pre-interview explanations about the identity of clients and procedures available for the interviewees to obtain further information.

Two possible scenarios based on real life practice (although neither of these have occurred in reality) illustrate the complexities faced by our industry relating to ownership of data:

- An online research project with a survey designed and deployed by company X uses panellists who have been paid to give their opinions supplied by company Y as interviewees.

The end client, company Z, releases a de-identified data file publicly that via meta data analysis by company P re-identifies information making it possible to establish personal information of online panellists provided by company Y. The end client, company Z, only has access to de-identified data. Company Y does not have access to the survey responses. Company X may still have the personally identified data (although it might already be de-identified) and was not responsible for the data breach. Company P caused the data breach.

- A government department that is part of an alliance of departments and organisations has provided the contact details of its customers to a market and social research company for the purposes of a research study in the public good. Some of the behaviours and attitudes investigated in the study are uncommon and participants are asked their willingness to participate in further, more specific research. The vast majority agree to this and are told that there is a possibility that another research company or agency will re-contact them for this purpose, but that the market and social research company will retain their records confidentially and securely. A sub sample of people who meet specific criteria is sent to a specialist SME with a turnover of less than $1,000,000 for follow up research and again the vast majority of people who are re-contacted agree to the research process. The data file is returned to the government department erroneously in an identified format and because of the nature of the project it is possible to determine sensitive facts about the individuals, which were not captured by the SME per se.

Question 5: Are there any other ways in which the draft resources could be enhanced?

In summary, the following areas could be expanded:

a) 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.
b) More emphasis on the need for documented prevention and notification procedures being embedded in organisations handling personal data.
c) Some practical advice about industry best practice such as separation of names and unique identifiers from other personal data.

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