AMSRO
ASSOCIATION OF MARKET AND SOCIAL RESEARCH ORGANISATIONS

Ten steps to privacy compliance

Working under the Market and Social Research Privacy Code 2014 (M&SRPC)

The following steps provide some guidance on the issues organisations should consider in developing a Privacy compliance program.

Introduction:

In dealing with the public and with any information entrusted to our care by them or for them, AMSRO members should remember that our industry relies largely on their good will. When following the steps in this list, therefore, members should always keep the best interests of the individual respondent in mind. Although privacy legislation relates only to personal information on private individuals, the market and social research industry treats all respondents with equivalent care and respect.

1. Appoint a Privacy Officer

Organisations should appoint a staff member to act as its privacy officer. The privacy officer should implement and oversee a privacy compliance strategy and respond to privacy enquiries and complaints.

2. Training about the Australian Privacy Principles (APPs) and the industry privacy code

Organisations should ensure its staff are familiar with the APPs and the Code and are aware of how they impact on its business practices. Training on the privacy laws and the privacy policy should be provided to all staff within the organisation.

See www.amsro.com.au/privacy for further information and tools.

3. Conduct an internal privacy review

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

4. Update and maintain your organisation's privacy policy

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

5. Update your organisation's privacy collection statements

Update the collection statement to comply with the Code and APP5 to align with the manner in which it uses and discloses personal information.

See M&SRPC APP5 and www.amsro.com.au

6. Conduct Privacy Risk Assessments (PIA) for new projects

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

In respect of any project to be undertaken, a threshold assessment should be conducted to assess whether your organisation will be collecting, using or disclosing any personal information. If the answer to this question is 'yes', your organisation should undertake a PIA to identify and assess possible privacy issues.

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

7. Prepare privacy procedures and security

Organisations should prepare policies and guidelines in respect of:

- The collection, management and use of contact lists;
- Provisions to deal with privacy in respect of any outsourcing or supplier contracts where personal information may be handled;
- Data security practices and procedures (including encryption, firewalls, restricted access and regular password changes, anti-virus software and backups to be stored securely in a separate location); and
- The removal, destruction or de-identification of data that is no longer required.

8. Develop an inquiry and complaint program

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

For members working under the M&SRPC please refer to www.amsro.com/privacy reporting procedures.

9. Conduct regular audits.

Audits should be conducted (outside of your annual ISO 20252 or ISO 26362 audits) at regular intervals to review what steps your organisation currently takes to ensure personal information is up to date, complete and accurate and in respect of disclosure that it is relevant. It's imperative that organisations review what steps are currently taken to ensure personal information collected is protected from misuse, interference, loss and from unauthorised access, modification or disclosure. See M&SRPC APP11.

10. Report potential breach to AMSRO

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

Members are required to advise AMSRO in regards to any serious or systemic complaints received and/or breaches that remain unresolved.

For further details on our data breach process please contact AMSRO Secretariat on (02) 9552 4618 or email amsro@amsro.com.au or visit the member section at www.amsro.com.au/privacy