Research News

Australian Market & Social Research Society | Volume 31 | Number 2 | March 2014

Privacy

ISSN: 1839-4256

Australian MARKET & SOCIAL RESEARCH SOCIETY | AMSRS

Changes to the Privacy Act and your business

KEY RECOMMENDED STEPS TO PREPARE FOR THE APPS

- Update privacy policy (APP 1)
- Develop an inquiry and complaint handling procedure (APP 1)
- Update all privacy collection statements (APP 5)
- Review cross border disclosures of personal information by the organisation to determine what changes will be required (APP 8)
- Review security measures for personal information to protect the information from interference (APP 11)

From the RICA privacy webinar, courtesy of HR Legal

The Australian Privacy Act sets out minimum standards for the collection and handling of identified personal information. Organisations conducting market or social research must be aware of these standards when they collect, use, disclose and store personal information in such a way that the individual who provided the information can be identified.

The new Australian Privacy Principles (APPs) come into force on 12 March 2014, replacing two set of principles – the National Privacy Principles (NPPs), covering organisations, and the Information Privacy Principles (IPPs), covering government agencies.

The APPs apply to all public and private sector businesses with a turnover of more than $3m per annum, and while most are based on the existing NPPs, there are some changes.

If the APPs apply to you, you need to review your organisation's processes and implement any changes required under the new APPs. A checklist is available from the Office of the Australian Information Commissioner (OAIC) to help you.

Changes that may affect your business

For the first time an APP (7) deals specifically with direct marketing. It states that an organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. If your company does any form of direct marketing in addition to market or social research, you must make sure these conditions are met. As always, ensure that the research you conduct is clearly differentiated from any other activities.

The Privacy Principles have always stated that a business can only send personal identified data to another country if that country has privacy legislation which is similar to that in Australia. A new APP (8) makes the business more accountable.

If your company sends identified data to another country in any format you must take rea-

sonable steps to ensure that the recipient does not breach the APPs and you may be responsible for any breach by that recipient.

Another major change is that the OAIC now has greater enforcement powers and can seek greater penalties for breaches of the Privacy Act – penalties of up to $1.7million.

Remember, the APPs only apply to personal information that could identify a person. We recommend that you de-identify any data that you have collected as soon as practically possible after your research project is complete. That means not only removing the name, but any other details that may identify the person: demographic characteristics, photos or videos, customer details and so on.

For more information

AMSRS will be developing a fact sheet to provide more detail on the APPs which will also be covered in the 2014 QPMR webinar on standards and regulatory issues.

AMSRO member enquiries regarding the Market and Social Privacy Code please contact AMSRO on (02) 9552 4618.

In the meantime, the OAIC website is the best source of general information http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform

AS A MARKET AND SOCIAL RESEARCH BUSINESS...

1. **Do** ensure appropriate systems and processes are in place to comply with the APPs.
2. **Don't** collect more personal information than is necessary or relevant.
3. **Do** tell individuals what you are going to do with the collected information.
4. **Don't** use information for a secondary purpose without consent.
5. **Don't** disclose personal information unnecessarily.
6. **Do** give people access to their personal information if they ask – unless there are proper grounds not to.
7. **Do** keep information secure and free from interference.
8. **Don't** keep personal information you no longer need or are no longer required to retain.
9. **Don't** disclose information to overseas recipients in countries without equivalent privacy laws and the ability to enforce those rights unless consent is provided.
10. **Do** make someone in the organisation responsible for privacy complaint handling, processes and systems.

Source: HR Legal, courtesy of AMSRO

AMSRO
ASSOCIATION OF MARKET & SOCIAL RESEARCH ORGANISATIONS