Australian Government
Office of the Australian Information Commissioner

Privacy business resource 9

Ten tips to protect your customers' personal information

May 2015

The *Privacy Act 1988* (Privacy Act) contains 13 Australian Privacy Principles (APPs) that Australian and Norfolk Island Government agencies, and most private sector organisations, (collectively called 'APP entities') must follow when they handle personal information. Personal information is defined in the Privacy Act as information or an opinion that identifies, or could identify, an individual. Some examples are name, address, telephone number, date of birth, medical records, bank account details, and opinions.

This ten tip guide will help you comply with the APPs when you handle your customers' personal information.

1. Familiarise yourself with internal privacy policies, processes and procedures

Understand your personal information handling processes and procedures and undertake regular privacy training. Following internal processes and procedures will help you manage and mitigate privacy risks, including the risks posed by human error.

Read your privacy policy and ensure you understand how it applies to the way you handle personal information.

Make sure you provide privacy notices to customers and that you handle their personal information in the way you say you will.

2. Know who is responsible for privacy

Everyone has a role to play in ensuring privacy is respected and protected. There should be a senior member of staff with overall accountability for privacy. There should also be staff responsible for managing privacy, including a key privacy officer, who:

- understands your entity's responsibilities under the Privacy Act
- handles access and correction requests and complaints and enquiries about your personal information handling practices.

If your workplace is small, the key privacy officer may hold this role as part of their broader responsibilities.

If you notice any issues with privacy processes and procedures, discuss it with the key privacy officer or someone senior.

3. Consider privacy during project planning

When developing a project that involves new or changed personal information handling practices, always consider doing a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy, and makes recommendations for managing, minimising or eliminating privacy impacts.

You should also engage your key privacy officer during the planning phase of your project.

More information can be found in the *Guide to undertaking privacy impact assessments*.

4. Only collect the personal information you need

You must only collect personal information that you actually need. Don't collect personal information just because it may become necessary or useful at a later date. If you need it later, you can collect it then.

You are also required to let people interact with you anonymously or through the use of a pseudonym (although some exceptions apply). Remember, you can sometimes conduct your business activities without collecting personal information.

5. Use and disclosure — think about it!

Generally, you are only allowed to use or disclose personal information for the primary purpose for which it was collected. However, there are exceptions that allow for it to be used or disclosed for another purpose. These exceptions include where:

- the individual has consented to the use or disclosure
- the individual would reasonably expect the use or disclosure and the other purpose relates (or for sensitive information, directly relates) to the primary purpose of collection
- the use or disclosure is required or authorised by law.

Always think about whether you can conduct your business activities without using or disclosing personal information. When you do, always limit the amount of personal information you use or disclose to the minimum necessary.

6. Overseas disclosure — prepare for it!

Before you disclose personal information to an overseas recipient, you must take reasonable steps to ensure that the recipient complies with the APPs (although there are some exceptions, which are outlined in APP guidelines Chapter 8). These may include entering into an enforceable contractual arrangement that requires the overseas recipient to handle the personal information in accordance with the APPs (except for APP 1).

If you disclose personal information to an overseas recipient you may remain accountable for how it is handled by that recipient (although again there are some exceptions).

More information can be found in *Sending Personal Information Overseas*.

7. Take care when handling sensitive information

Sensitive information is given a higher level of privacy protection under the Privacy Act and you have additional responsibilities when you collect, use or disclose it.

Sensitive information is a specific set of personal information that includes an individual's racial or ethnic origin, religious beliefs or affiliations and sexual orientation or practices. It also includes information about health, genetics and biometrics. Generally, sensitive information can only be collected with someone's consent.

8. Access personal information on a need-to-know basis

Generally, you should only have access to personal information that you need for your role or function. By limiting the personal information you and your staff access to that needed, you are helping to protect the information from unauthorised access, use or disclosure.

9. Keep personal information secure

You must take reasonable steps to protect personal information from unauthorised access, modification or disclosure and also against misuse, interference and loss. You must also take reasonable steps to destroy or de-identify personal information when it is no longer needed for any purpose permitted under the Privacy Act. This requirement does not apply if you are required or authorised by law to keep it.

Make sure you are familiar with and follow your policies on information security, including ICT security, physical security and access security. Always destroy and de-identify personal information in accordance with your destruction policies.

More information about information security can be found in the *Guide to securing personal information*.

10. Familiarise yourself with your data breach response plan

All entities should have a data breach response plan. Make sure you are familiar with your data breach response plan, as this will help you respond quickly and appropriately in the case of a data breach. A quick response can substantially decrease the impact on the affected individuals. It is also best practice to notify the OAIC when you have a data breach and there is risk of serious harm to the affected individuals.

If you don't have a data breach response plan, our *Data breach notification — A guide to handling personal information security breaches* will help you in preparing for and responding to a data breach.

Don't leave privacy to chance.

For further information

For more information about the APPs, see the OAIC's Australian Privacy Principles guidelines and Fact sheet 17 – Australian Privacy Principles

For more information about which private sector organisations are covered by the Privacy Act, see the OAIC's Private sector organisation exemptions

The information provided in this resource is of a general nature. It is not a substitute for legal advice.

telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
Or visit our website at www.oaic.gov.au