Australian Government

Office of the Australian Information Commissioner

October 2016

Handling privacy complaints

www.oaic.gov.au

Contents

This resource will help organisations and agencies covered by the *Privacy Act 1988* (Cth) (Privacy Act) address privacy complaints they receive.

Are you covered by the Privacy Act?

Under the Privacy Act, businesses (including non-profit organisations) with an annual turnover of more than $3 million, some small businesses (including all private health service providers) and most Australian Government agencies must comply with the Australian Privacy Principles (APPs).[1]

An alleged breach of the APPs can be investigated by the Australian Information Commissioner (Commissioner).

As well, some other interferences with privacy, for example in relation to the handling of consumer credit reporting information, tax file numbers or spent conviction information, can be investigated by the Commissioner. Some additional organisations (to those covered by the APPs) are subject to these obligations.

More information on whether your organisation or agency is covered by the Privacy Act is available on our Rights and responsibilities webpage.

When is your organisation/agency involved?

The Privacy Act says that an individual who considers that an organisation or agency has interfered with their privacy should make their complaint to that organisation or agency first and allow an adequate opportunity for the complaint to be dealt with by the organisation or agency (generally giving 30 days for a response).

If not satisfied with the response the individual may, if the complaint is about an organisation, take their complaint to a relevant external dispute resolution (EDR) scheme of which the organisation is a member.

The individual may then make their complaint to the Commissioner if: an EDR scheme is not an option; if the individual is not satisfied with the outcome of an EDR process; if the individual would prefer to complain directly to the regulator; or if the complaint is about an agency.

How does the OAIC handle privacy complaints?

Where appropriate the Commissioner can make preliminary enquiries into the matter, investigate and/or attempt to resolve the complaint by conciliation.

The Commissioner also has the power to decline to investigate complaints (or not to investigate further) in a number of circumstances, including where:

[1] For help in interpreting the APPs in the Privacy Act see the OAIC's APP guidelines.

- it is clear that there has not been an interference with privacy
- the matter has been, or is being, adequately dealt with by the organisation/agency or a recognised EDR scheme, or
- it has been more than 12 months since the complainant became aware of the issue that may be an interference with privacy.

If a complaint is not resolved, or is not finalised on some other basis, the Commissioner may make a determination about whether an interference with privacy has occurred.

For more information, see the OAIC's Privacy Regulatory Action Policy and the Guide to OAIC Privacy Regulatory Action — Chapter 1: Privacy complaint handling process.

How does your organisation/agency handle privacy complaints?

Consider the following:

- Is it easy to make a privacy complaint to your organisation/agency? For example:
  - Is information about who to contact to make a privacy complaint easy to find?
  - Does your organisation/agency have feedback or complaint forms in print and electronic formats?
- Are privacy complaints identified and directed to staff with appropriate knowledge of the Privacy Act?
- Consider whether it is possible to resolve a privacy complaint informally by talking to the individual and, if appropriate, providing an explanation and/or apology.
- Are there regular reviews of the issues raised by privacy complaints (including in relation to your complaint handling procedures)?
- Does your organisation/agency have a data breach policy and response plan (that includes consideration of whether to notify affected individuals and the OAIC of a data breach)? Being prepared to react to data breaches may assist to mitigate damage to the affected individuals, and avoid potential complaints. The OAIC has published a guide to handling personal information security breaches that deals with how to effectively prepare for and respond to data breaches.

Below is a checklist to help your organisation/agency address privacy complaints.

Checklist for addressing privacy complaints

Preliminary steps

1. Is the complaint about the organisation or agency's handling of an individual's personal information?[2]

COMPLETED ☐

- ☐ **Yes**. Treat as a privacy complaint, and go to Question 2.
- ☐ **No**. Follow the organisation or agency's usual complaint handling procedures.

2. Is the personal information involved in the complaint the personal information of the individual making the complaint?

COMPLETED ☐

- ☐ **Yes**. Go to Question 3.
- ☐ **No. If not, do you know if the complainant represents the individual whose personal information the complaint is about?**[3]
  - ☐ **Yes.** Go to Question 3.
  - ☐ **No.** Clarify the complainant's authority to act for the individual whose personal information the complaint is about. If you go ahead without the proper authority, you risk disclosing personal information and you may be in breach of APP 6 and APP 11.

3. Does the complaint involve any of the following?

COMPLETED ☐

- ☐ Collection of personal (including sensitive) information (APP 3).[4]
- ☐ Use and/or disclosure of personal information (APP 6).
- ☐ Accuracy of personal information (APP 10).
- ☐ Security of personal information (APP 11).
- ☐ Refusal to give access to personal information (APP 12).
- ☐ Refusal to correct personal information (APP 13).
- ☐ Other APP issues.
- ☐ Other interferences with the complainant's privacy. There are a number of other privacy interferences that are covered by the Privacy Act or subject to investigation by the Commissioner. For more information on what the Privacy Act covers and/or what the Commissioner can investigate see our Rights and responsibilities webpage.
- ☐ Unsure. If you are not sure, go back to the complainant and seek further information.

If the complaint is not one to which the Privacy Act applies or the Commissioner can investigate, consider whether you can deal with the matter under the organisation or agency's usual complaint handling procedures.

4. Contact the complainant to advise:

COMPLETED ☐

- ☐ Your understanding of the conduct complained about.
- ☐ Your understanding of the privacy obligations at issue, for example the particular APPs (if appropriate).
- ☐ That the organisation/agency is conducting an investigation (if appropriate).
- ☐ The name, title, and contact details of the staff member handling the complaint.
- ☐ How that staff member is independent of the person/s responsible for the alleged conduct.
- ☐ A request that the complainant outline what they expect as an outcome.
- ☐ When you will contact the complainant again.

Investigating the issues raised

5. Matters to consider:

COMPLETED ☐

- ☐ Does it appear that the alleged conduct occurred?
- ☐ Which privacy obligation/s may be relevant and why?
- ☐ Does it appear that the conduct complied with the organisation or agency's privacy obligation/s (taking into account any exceptions or exemptions under the Privacy Act or other legislation)?
- ☐ If it appears the organisation or agency has not complied with their obligations, consider whether the complainant's requests regarding outcomes can be met.
  Examples of outcomes may be: An apology, a change in procedures, improvement of security safeguards, payment of compensation for loss or damage suffered.

Communication with the complainant

6. Your response to the complaint

COMPLETED ☐

- ☐ If possible, call the complainant first and then follow up in writing providing your response to the complaint. Include details about the information you have relied on in developing the response.
- ☐ Include an invitation for the complainant to reply to your response and if appropriate, the offer of a meeting or discussion.
- ☐ Include an apology if you did not comply with the relevant privacy obligation/s and consider whether any additional outcomes may be appropriate.

7. Complainant's reply

COMPLETED ☐

- ☐ Assess any reply or further information from the complainant.
- ☐ If you initially found that the organisation or agency did comply with its privacy obligation/s, does the complainant's response alter your view?
- ☐ Consider if an external mediator may be helpful to resolve the matter.

If the complainant remains unsatisfied with the outcome, refer the complainant to your EDR scheme (if it deals with privacy issues) or, if you are not a member of an EDR scheme, to the OAIC.

Systemic issues

8. Consider any systemic issues raised by the complaint and possible responses, such as:

COMPLETED ☐

- ☐ Privacy training
- ☐ Amendment of policies, forms and/or collection notices
- ☐ Providing additional accessible information
- ☐ Improve security and storage measures
- ☐ Steps to improve data accuracy

Make a record of any changes made.

Evaluate the changes within 12 months as well as against any future privacy complaints.

Finalisation

9. Storage

COMPLETED ☐

- ☐ When finalised, the record of the complaint and the investigation and outcome should be stored securely (APP 11) and in accordance with your organisation or agency's record keeping requirements.

[2] 'Personal information' is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not'.

[3] If the complaint is from a Member of Parliament on behalf of a constituent or from a lawyer on behalf of a client, it is assumed that the individual has consented for the writer to act on their behalf. In all other circumstances, you should check that the writer has the complainant's consent to act on their behalf.

[4] 'Sensitive information' is an important category of personal information. Sensitive information includes information of an opinion about an individual's health, genetic or biometric information, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record. The Privacy Act imposes stricter rules about when sensitive information can be collected and how it should be handled. Usually, sensitive information can only be collected with the individual's consent and there are tighter restrictions on how this type of information can be used and disclosed.