



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/About/Contacts.htm>

16 December 2013

By email: consultation@oaic.gov.au

Re: DRAFT APP GUIDELINES 12 and 13

The Australian Privacy Foundation (APF) is pleased to provide comments on the draft Guidelines for the Australian Privacy Principles 12 and 13.

APF has had the opportunity to review the submission of the former Deputy Privacy Commissioner, Nigel Waters and are generally supportive of the points made in his submission.

General Comments

The general comments made in our previous submission still apply to Guidelines 12 and 13. Our previous submissions are available at <http://www.oaic.gov.au/privacy/privacy-engaging-with-you/current-privacy-consultations/draft-australian-privacy-principles-guidelines/submissions-on-the-draft-app-guidelines-2013>.

APP 12

General comments

APP12 needs redrafting as it is confusing particular for the private sector. It is attempting to cover access to personal information for commonwealth government agencies and APP entities. For agencies the FOI requirements apply. For organisations the FOI requirements are not relevant. The Guideline needs to be clear exactly how the requirements apply and when. In particular, the mixing of reference to agencies and organisations needs to be separated with clear headings.

It should be possible and easy for an individual, organisation or agency to clearly identify what parts of the guideline are relevant to them. As it currently stands, it is very difficult to access clear guidance on the requirements on access to personal information.

The other general comment relates to the practicality of the guideline. The major issues for individuals are:

1. That the process for getting access to personal information is easy and straightforward; and
2. The individual is not charged excessive costs; and
3. The individual is not unreasonably refused access.

The Guideline needs a lot more practical guidance on making sure that the individual gets access to their personal information.

What does APP12 say?

The last sentence of this section refers to the suitability of processing an information request under FOI rather than APP 12. The obvious question unanswered here is why it would be suitable and when? This question needs to be answered. It is also of concern that any individual may be talked into giving up rights under APP 12.

'Holds'

This section does not cover the issue of multiple APP entities holding personal information. It is our understanding that this is commonplace in related APP entities.

Verifying an individual's identity

A common problem for an individual is that in trying to get access to their own personal information the identification requirements are so onerous as to be intrusive. Individuals can be asked for multiple types of photo identification just to get access to their own personal information. The irony is that the individual's privacy is endangered as they give over photo identification that may be held and dealt with inappropriately by the APP Entity.

The Guideline needs to provide detailed guidance on what is reasonable to request in terms of identification.

We suggest:

1. A signature and identifiable details that can be cross checked for individuals who already have a relationship with the APP entity
2. If new identification is being used to verify identity it must always be sighted only (with a note about the sighting) and never copied
3. If copies are sent by the individual of their identification then the copies must be destroyed or returned
4. A request for photo identification only as acceptable is onerous and inconsistent with privacy rights

Giving access under APP 12 – processing requirements

This section is confusing because it moves between organisations and agencies. It needs to be clear how each of the comments apply. The interaction between agencies, APP 12 and FOI needs to be explained in an introductory paragraph.

An important objective for individuals is that they are not “unreasonably” refused access to their personal information.

The most important point is that individuals should not have to follow a detailed procedure set out in a privacy policy buried on a website. No matter how the individual contacts the APP entity it must respond to that request. This point should be clear in the Guideline.

Paragraph 12.19 seems to be unnecessarily narrow. It would appear from this paragraph that individuals would need specialist legal advice to make sure they request access under the correct access regime. As there is no free specialist legal advice available we contend that any request for access by an individual should be processed under whatever regime may apply (e.g. FOI and APP 12). The Guideline should state that:

- a person who just requests access should be processed under both regimes
- if another point of access is available the individual should be advised about this

Paragraph 12.20 is not helpful at all. Individuals are very unlikely to read 13 guidelines to find this section giving the circumstances when it “may be preferable for an individual to make an access request under FOI. As stated above, an individual should not need legal advice to access their personal information under FOI and/or APP12. If this section is going to be maintained it needs to find its way into a fact sheet. The section is also misleading about the individual’s rights in the event of refusal. It is unclear why the individual’s rights under the Privacy Act have disappeared.

The matters set out in this section are subject to misuse so it is very important that the reasons for refusal are narrowly defined. We recommend that the Guideline should include a series of common examples/case studies where it would be unreasonable to refuse access.

When an agency may refuse to give access under APP 12

This section deals with FOI requests to an agency. It does not cover the interaction between APP 12 and FOI in any clarity. This section has the potential to mislead as the reader of the Guideline may believe that an FOI refusal would be the end of an attempt for access.

Authority to refuse access under the FOI Act

We also refer to bullet point 2 of 12.24 which appears to need further detail. This reason for refusal could be used inappropriately to deny access. This section needs examples and further clarity.

Required or authorised to refuse access under another Act

If the agency is relying on this section it must be required to specifically reference under what sections of what Acts it is refusing access.

When an organisation may refuse to give access under APP 12

Giving access would have an unreasonable impact on the privacy of other individuals

This section needs to be very detailed otherwise it could be used as a reason to refuse many requests for access.

It is also important to avoid the use of redaction as an option as the request for access will come back all black with only a few words that mean nothing.

Case studies should be used here to demonstrate situations when it would be unreasonable to refuse access.

The information requested relates to an existing or anticipated legal proceeding

This section needs to be clearer about what is meant by the process of discovery. Several small claims divisions of courts do not have a formal process of discovery. This may then create a loophole where a request for personal information may be unreasonably denied. This part needs to be clarified.

Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct

Unfortunately, even with the list of requirements in the Guideline this section is not drafted narrowly enough to prevent unreasonable misuse of this section.

In order to clarify this matter, the meaning of prejudice needs to be clarified in paragraph 12.50 to narrowly define what the prejudice would be.

Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct

It is unclear on why the test of “reasonably believed” would lower and change at all.

APP 12 minimum access requirements

This section needs to provide practical guidance on how to make access to personal information easy, straightforward and in a streamlined way. Instead this section has concentrated on a negotiation process for providing access.

The hardest task for an individual in requesting access to personal information is finding the best way to ask. Being referred to a small print privacy policy buried on a website is not an easy way to get access to personal information. Minimum standards should be set on how the individual should be:

1. Able to contact the organisation and expect a response
2. Able to have any letter sent referred to the appropriate section for response

These minimum standards should be specified in the Guideline.

Access charges

A common way for organisations to thwart access to personal information is to impose excessive charges for access to personal information. It is often arguable about what the actual cost is. Many organisations seem to want to factor in a whole range of pro rata costs in working out the actual costs. The actual costs need further specification. For example, the photocopying charges can be calculated based on the cost of paper and the depreciation of the state of the art photocopying machine when the actual cost is arguably a few cents a page.

It may be appropriate for the OAIC to provide further specific guidance in another document.

Giving written notice where access is refused

We contend that 12.77 should include an extra dot point to require any steps that may be taken by the individual that would mean that access is not refused (if applicable).

APP 13 – correction of personal information

General comments

Being able to easily correct inaccurate personal information is extremely important for individuals. Inaccurate information can cause individuals enormous detriment including being sent court documents to an incorrect address. It is essential that information can be corrected simply and easily. It is also critical that once the information is corrected the individual is notified in writing of that correction.

We also reiterate the comments that applied to APP 12 in relation to the confusion between organisations and agencies. The comparison between APP 13 and FOI procedures is confusing and unclear and needs to be rewritten.

We suggest that case studies are incorporated into this APP Guideline to demonstrate the points.

Thank you for your consideration.

Yours sincerely

Katherine Lane
On behalf of the Board of the Australian Privacy Foundation
P: 02 82041350
E: kat.lane@cclcnsw.org.au