WEBSITE - FAQ'S

We have detailed below a number of frequently asked questions or **FAQ's** for you to consider.

In no particular order, you may wish to consider the following matters:

1 Employment agreements

Do we need to address our employment contracts to cover:

(a) Employee's responsibility to comply with Privacy legislation (in relation to their dealings with clients and potential clients); and/or

(b) addressing the personal information collected from them via their employment arrangements?

Generally, employment contracts will require employees to comply with legislative requirements and all reasonable directions from their employer (including having to comply with company policy).

You could add an additional clause, if you wish, to highlight employee obligations in relation to the handling of personal information.

One of the areas of focus for the Privacy Commissioner is for organisations to develop ongoing practices (including training where appropriate) and policies to ensure that personal information is managed in an open and transparent way.

The intention is that those practices and polices be reviewed regularly to ensure they address any changes your firm may implement in practice.

Of course, employee records themselves are exempt under the Act. However, that exemption does not extend to other service providers such as temps and independent contractors.

Similarly the exemption does not extend to personal information which is not related to the employment relationship.

2 Direct marketing

Can we assume that we are entitled to send direct marketing material to all clients and contacts?

APP 6 provides that an organisation must not use information for a secondary purpose unless the individual consents or an exception applies.

APP 7 further provides that the use and disclosure of personal information for direct marketing is prohibited unless an exception applies. The exceptions highlight the need to identify the source of the information.

If information is collected directly from an individual, with their consent, the information may be used for direct marketing if:

- The individual would reasonably expect the information to be used for direct marketing (which you could infer for most clients and could also address by way of your privacy policy and terms of retainer, as we previously proposed);
- A simple opt out method is provided (which is also a requirement of the SPAM Act for electronic communication); and
- The individual has not previously requested to opt out.

If personal information is collected from an individual who would not expect it to be used for direct marketing or if the information is collected from a third party then it may only be used where:

- The individual has consented or it is impracticable to obtain that consent;
- A simple opt out method is provided;
- The individual has not previously requested to opt out; and
- In every marketing communication (including hard copy) a prominent opt out statement is made (APP 3).

Sensitive information (e.g. racial origin, political or religious beliefs and health information) should only be collected with an individuals consent (APP 6) and may only be used for direct marketing if consented to (APP 7.4).

Under APP 7.6 and 7.7 a person may request an organisation to disclose the source of information and that must be done within a reasonable period, unless impracticable or unreasonable to do so.

3 Recording sources of information

What steps do we need to take to record the source of data?

The Privacy Commissioner has suggested that organisations should conduct a review (audit) of the personal information which they hold and whether there are systems in place to address the collection and use of that material.

The Act requires that you assess all unsolicited information and consider whether you are able to obtain that information under the collection requirements set out above. If so, then the information must be dealt with in the same manner as all other personal information. If none is recorded, then that is not an issue.

If you obtain the client's consent to the collection of the information you may also wish (at the same time) to obtain their consent to you using the information for direct marketing.

If you are providing personal information to third parties (e.g. Associated firm, consultant, contractor, lawyer or related party of a client) you should ensure that you have clear instructions/consent.

4 Publically available information

What are our obligations in relation to information obtained from public databases – e.g. ASIC searches, Dun & Bradstreet, White Pages.

The fact that information is publicly available (including via those various databases) will not prevent it from being regarded as personal information if compiled by you into a database or list.

The strict position is that organisations must take reasonable steps to implement new practices, procedures and systems that will ensure compliance. As you know a civil penalty regime has been introduced which provides for fines of up to $1.1 million for companies who are serious or repeat offenders. You most definitely should endeavour to note the source of the information prospectively. It is difficult to know whether the Privacy Commissioner will allow any latitude in relation to information collected prior to the commencement of the new provisions. However, if a query is raised, we would suggest that the Privacy Commissioner would take into account the steps taken to ensure compliance with the new requirements and in relation to the policies and procedure adopted by an organisation, particularly in regard to the collection, handling and use of personal information. The mechanisms adopted for handling of complaints may also be relevant, particularly if individuals have made requests which have not been responded to or acted upon.

The Privacy Commissioner has confirmed (in their compliance materials) that you should not disclose personal information to another organisation for them to send unsolicited direct marketing without the individual's permission. That would likely include any affiliated bodies and should be addressed in your privacy policy and retainer, if necessary. If in doubt, you can ask an individual for consent to send direct marketing material to them when or as soon as possible after collecting their information. The principle also works in reverse for any information which you collect from another party (in relation to 3rd parties). It may be prudent for you to review your policy documents and letter of engagement or initial letter to client. Please let us know if you would like us to assist in that regard.

APP 5 requires that reasonable steps are taken to notify an individual or otherwise ensure that an individual is aware:

- That its APP privacy policy contains information about how to access and seek collection of personal information, and information about the complaints process (APP 5.2(g) & (h));
- Of whether it is likely to disclose an individual's personal information to overseas recipients and, if practicable, to specify the countries in which those recipients are likely to be located. If it is not practicable to specify the countries in the notification, you may make the individual aware of them in another way.

Under APP 7.6 and 7.7 a person may request an organisation to disclose the source of information and that must be done within a reasonable period, unless impracticable or unreasonable to do so.

As an example, the OAIC has indicated that it will take a similar view in relation to information collected by a purchaser which is undertaking a due diligence of the purchase of a businesses assets including customer databases. In that case, the purchase must take steps to ensure compliance with the new requirements.

The source of the information should be recorded on collection. For example, organisations which are subject to the APP are required to implement practices, procedures and systems which ensure compliance with the APP and allow them to deal with complaints from individuals. As noted previously, (and further discussed below), APP 5 requires that you notify an individual of the circumstances of the collection of their personal information (in addition to the fact of collection). The circumstances of collection include detail regarding the source of the information.

Also, where the individual whose personal information you hold may ask for you to disclose the source of the information collected, that standard (of recording the source of information) is clearly implied and appears to be a pre-requisite to good practice.

APP 5 provides that the individual must be notified at as before the time personal information is collected and if that is not practicable then the individual whose personal information has been collected should be notified as soon as practicable thereafter. The rationale is that it is preferable for an individual to be able to make an informed choice about whether to provide personal information to an entity. Notification could be excused in some circumstances. The guidelines cite an example being where a doctor informs a patient that a specialist will collect their personal information following referral.

5 What about social media and collection from public databases?

Information collected from a public database may be permitted in most cases (the principles say information must be collected from the individual unless it is unreasonable or impractical to collected from the individual).

Depending on the nature of the information collected and where it is published, there may also be a reasonable expectation that it would be used for certain purposes. That might be easier to argue in some cases. For example, if an individual has a LinkedIn page or corporate website (with contact details) they may more readily anticipate use than if the information appears on a private site/account.

6 Information obtained by others

What are our obligations in relation to Information obtained by others during the course of providing services, for example, a contractor who obtains personal details while providing a service?

In that case, the personal information must be handed in accordance with the collection requirements under the Act.

You will also need to comply with the Security requirements under APP 11 to ensure that the information is protected from misuse, interference, loss or unauthorised access.

You should also consider when the information can be destroyed or de-identified if no longer needed, in accordance with APP 11.

7 Information transmitted offshore

What steps do we need to take when personal information is disclosed offshore?

Although you do not need express consent from customers or clients to enable another party to access their personal information offshore, the Act requires that you be transparent about the use/disclosure of (client's) information offshore.

If your clients provide consent to cross-border disclosure, then APP 8 will not apply. That can be dealt with via your privacy policy, or via your client engagement.

The structure of the offshore contract and likely disclosure are relevant.

8 Data breaches

The Notifiable Data Breach (NDB) scheme requires entities to notify affected individuals and the Privacy Commissioner where a data breaches occurs involving personal information that is likely to result in serious harm to any individual affected.

It is important to understand that data breaches don't just occur as a result of hacking, but can occur from simple human behaviour leading to accidental loss or disclosure of personal information. Examples of data breaches include the following incidents:

- a device containing customers' personal information is lost or stolen – such as a mobile phone being left/lost; or
- personal information is mistakenly provided to the wrong person – which could be as simple as putting the wrong letter in the wrong envelope or sending an email to the wrong recipient.
-

Who must comply with the NDB scheme?

Any organisations which must comply with the *Privacy Act 1988* will be bound by the NDB scheme. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of $9 million or more. Some organisations such as credit reporting bodies and health service providers must comply even if they don't meet the $3 million threshold due to the sensitivity of the information which is collected.

What I need to do when there is a data breach?

When a data breach has occurred, organisations must promptly assess whether individuals are at likely risk of serious harm and whether steps could be taken to contain the breach. That must

be done promptly (within days rather than weeks). The Commissioner must also be notified as soon as practicable, if that is required.

The Privacy Commissioner highly recommends that organisations develop a Data Breach Policy so that they are not trying to establish protocols on the run in times of crisis. Whether organisations have developed a Data Breach Policy is also a matter that the Privacy Commissioner has flagged that they will take into account when assessing an organisation compliance with the Privacy Act and response to a data breach.

We haven't prepared a Data Breach Policy but you should let us know whether that is required.