PRIVACY IN THE WORKPLACE

The *Privacy Act 1988* (the Privacy Act) is intended to establish a comprehensive national scheme for the collection, holding, use, correction, disclosure and transfer of personal information by organisations in the private sector. This gives individuals the right to know what information an organisation holds about them and a right to correct that information if it is wrong. The *Amendment (Enhancing Privacy Protection) Act 2012* introduced 13 Australian Privacy Principles (APP) that have replaced the National Privacy Principles and Information Privacy Principles. The APP will be effective as of 12 March 2014.

Notable Changes

The amendments to the Privacy Act have made minor but important changes to the way information can be handled and the consequences of a breach. These include:

- Clarification on the sort of information that can be collected and held by an organisation. An organisation cannot collect or hold personal information without the informed consent of an individual. The individual must be made aware of the fact that the organisation is collecting their information, the reasoning and purpose behind the collection of the information, and any other individuals or entities to whom that information may be disclosed. Further, an organisation needs to ensure that an individual is aware that they can correct any information that is held about them.
- Organisations who wish to use an individual's personal information for the purpose of direct marketing should seek the consent of that individual for each occasion the information will be used.
- Organisations must now exercise caution when dealing with third party requests for information. Organisations must ensure they have clearly informed and gained consent from individuals to provide that individual's information to agencies, government bodies, courts, tribunals (etc) when required by law.
- The Privacy Commissioner now has the ability to investigate serious breaches of privacy, assess an organisations privacy performance and impose penalties of up to $11 million on businesses who have breached the Privacy Act.

Related Legislation:

- Freedom of Information Act 1982 (FOI Act)
- Do Not Call Register Act 2006
- Spam Act 2003

Summary of the Australian Privacy Principles

1 – Open and Transparent Management of Personal Information

An organisation must manage personal information in an open and transparent way. This principle aims to encourage organisations to better handle sensitive private information, and to assist in building community trust and confidence in those practices.

APP 1 imposes three main obligations on an organisation:

1. To take reasonable steps to implement practices, procedures and systems that will ensure that the organisation complies with the APPs and any binding registered APP code, and is additionally able to deal with related enquiries and complaints.
2. To ensure that organisations have a clearly worded and up-to-date privacy policy governing how they manage personal information.

3. To take reasonable steps to make sure that the Privacy Policy is available free of charge in an appropriate form and, upon request, in a particular form.

APP 1 requires that organisations plan and explain how personal information will be handled before it is collected. It is recommended that organisations embed privacy protections in the design of their information handling practices.

2 – Anonymity and Pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an organisation in relation to a particular matter.

This does not apply where:

1. The organisation is required or authorised under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves.
2. It is impracticable for the organisation to deal with individuals who have not identified themselves or used a pseudonym.

3 – Collection of Solicited Personal Information

The requirements for collecting solicited personal information vary depending on whether the personal information is classified sensitive information or not, and whether the organisation is an agency or not.

In summary, the principles that apply are:

- An organisation may only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities.
- An organisation may only solicit and collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies.
- An organisation may solicit and collect personal information by lawful and fair means and must do so directly from the individual unless an exception applies.

4 – Dealing with Unsolicited Personal Information

This principle ensures that personal information that is received by an organisation is afforded appropriate privacy protection, even where the organisation has not solicited the personal information.

Unsolicited personal information is personal information received by an entity that has not been requested. When an organisation receives unsolicited personal information, they must decide whether or not they could have collected the information under APP 3.

If the organisation could not have collected the personal information and the information is not contained in a Commonwealth record — the entity must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so.

Alternatively, if the entity could have collected the personal information under APP 3, or the information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the information because it would be unlawful or unreasonable to do so — the entity may keep the information but must deal with it in accordance with APPs 5–13.

An organisation should consider the following issues:

- Has the entity received unsolicited personal information?
- Could the entity have collected that personal information under APP 3?

- If the entity is an agency or a 'contracted service provider', is the personal information contained in a Commonwealth record?
- Should unsolicited personal information held by the entity be destroyed or de-identified, or should it be retained and dealt with in accordance with APP 5–13?

5 – Notification of the Collection of Personal Information

As soon as practicable, an organisation that collects personal information about an individual must take reasonable steps to either notify the individual of certain matters, or ensure that the individual is aware of those matters.

This applies to both solicited information and unsolicited personal information that has not been destroyed or de-identified.

6 – Use or Disclosure of Personal Information

An organisation should only use or disclose an individual's personal information in ways that the individual would expect, or where one of the exceptions apply. In other words, information should only be used for the primary purpose for which it was collected.

Exceptions include:

- The individual consented to a secondary use or disclosure.
- The individual would reasonably expect the secondary use or disclosure, and that it is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose.
- The secondary use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order.
- A permitted general situation exists in relation to the secondary use or disclosure of the personal information by the APP entity.
- A permitted health situation exists in relation to the secondary use or disclosure of the personal information by the organisation.
- The organisation reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

An organisation may disclose personal information, other than sensitive information, to a related body corporate.

7 – Direct Marketing

An organisation must not use or disclose the personal information it holds about an individual for the purpose of direct marketing. Exceptions apply where an individual would reasonably expect their personal information to be used for direct marketing, and where express consent has been given.

An organisation must provide a simple means by which an individual can request not to receive direct marketing communications. In circumstances where an organisation has not obtained personal information from the individual, or the individual would not reasonably expect their personal information to be used in this way, there are additional requirements to ensure that the individual is made aware of their right to opt out of receiving direct marketing communications from the organisation.

An organisation cannot use or disclose sensitive information about an individual for the purposes of direct marketing without express consent.

Where an organisation is a contracted service provider for a Commonwealth contract and the information has been collected for the purpose of meeting an obligation under that contract, an exception applies.

An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations. The organisation must give effect to any such request by an individual within a reasonable period of time and for free.

An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so.

This principle applies to the acts and practices of an organisation that are exempt from the *Do Not Call Register Act 2006*, and the *Spam Act 2003* or any other legislation prescribed by the regulations apply.

8 – Cross-Border Disclosure of Personal Information

Before an organisation discloses any personal information to an overseas recipient, they must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs.

When disclosing to an overseas recipient, an organisation should keep in mind that it can only disclose personal information for the primary purpose for which it was collected unless an exception to that principle applies under APP 6.

9 – Adoption, Use or Disclosure of Government Related Identifiers

This principle restricts the general use of government related identifiers so that they do not become universal identifiers. That could jeopardise privacy by enabling personal information from different sources to be matched and linked in ways that an individual may not agree with or expect. Government identifiers include tax file numbers, Centrelink reference numbers, and drivers licence numbers (etc).

Some government related identifiers are regulated by other laws that restrict the way that organisations can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.

An organisation must not adopt, use or disclose a government related identifier unless an exception applies. Individuals cannot consent to the adoption, use or disclosure of their government related identifiers.

10 – Quality of Personal Information

An organisation must take reasonable steps to ensure that the personal information it collects, uses and discloses is accurate, up-to-date and complete. This applies only where an organisation 'holds' the information.

11 – Security of Personal Information

An organisation must take a proactive approach to ensuring the security of personal information that it holds. It must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Where personal information is no longer needed for any purpose that it can be used/disclosed for under the APP, the organisation must take reasonable steps to destroy or de-identify the information. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information.

12 – Access to Personal Information

An organisation that holds personal information about an individual must, on request, give that individual access to the information.

This principle sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

For organisations, there are 10 grounds on which an organisation can refuse to give access to personal information. An organisation should consider whether censoring some information would enable an individual to access their personal information rather than refusing on the grounds below:

1. The organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual/to public health/public safety.
2. Giving access would have an unreasonable impact on the privacy of other individuals.
3. The request for access is frivolous or vexatious.
4. The information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings.
5. Giving access would reveal the intentions of the entity in relation to negotiations with that individual, and would prejudice those negotiations.
6. Giving access would be unlawful.
7. Denying access is required/authorised by or under Australian Law or a court/tribunal order.
8. The organisation has reason to suspect that unlawful activity or serious misconduct relating to the organisation has been engaged in, and giving access is likely to prejudice the taking of appropriate action.
9. Giving access would be likely to prejudice one or more enforcement related activities conducted by/on behalf of an enforcement body.
10. Giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.

APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an organisation from giving access to personal information under an informal administrative arrangement, provided the minimum access requirements stipulated in APP 12 have been met.

13 – Correction of Personal Information

An organisation must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

Special considerations apply to Commonwealth records. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with the legislation.

In regards to correcting personal information, an organisation must:

- Take reasonable steps to notify a third party of a correction made to personal information that was previously provided to that third party.
- Give written notice to an individual when a correction request is refused, including the reasons for the refusal and the complaint mechanisms available to the individual.
- Upon request by an individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.

- Respond in a timely manner to an individual's request to correct personal information or to associate a statement with the personal information.
- Not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement.

Contacting the Victorian Chamber of Commerce and Industry

The Victorian Chamber's team of experienced workplace relations advisors can assist members with a range of employment, human resources and industrial relations issues.

Our experienced workplace relations consultants can also provide assistance to both members and non-members on a range of more complex matters for a fee-for-service. The consultants can, among other things, provide training to employees, conduct investigations and provide representation at proceedings at the Fair Work Commission.

For assistance or more information, please contact the Workplace Relations Advice Line on **(03) 8662 5222.**

Disclaimer