



LANCIONE PARTNERS  
LAWYERS

---

## SCF CONTAINERS INTERNATIONAL PTY LTD

### Privacy Act

#### 1 EXECUTIVE SUMMARY

Many private sector organisations must comply with privacy obligations in relation to personal information about individuals which they collect, use and disclose. Those obligations are set out primarily in 10 National Privacy Principles (NPPs) contained in the *Privacy Act 1988 (Cth)* (Act). This paper explains some of the key terms used in the Act, summarises the NPPs and discusses their application. The last section in this paper provides a quick checklist of issues to cover.

The Act also regulates the collection and use of credit information and the information collection and handling practices of Commonwealth Government bodies.

#### 2 ACT OVERVIEW – KEY TERMS AND BASIC PRINCIPLES

##### 2.1 Meaning of key terms

To understand how the Act operates, it is important to understand some of the key terms used which are as follows:

- ◆ **Information Privacy Principles** (IPPs) – these 11 Principles are the Commonwealth Government sector equivalent of the NPPs.
- ◆ **National Privacy Principles** – these 10 Principles are the foundation of the private sector privacy regime. They cover aspects such as collection, use, accuracy, access, security and anonymity.
- ◆ **Organisation** - the Act applies to "organisations". The term is defined broadly and covers most private sector entities including natural persons, partnerships, companies, trusts and so on. Generally, governmental bodies are not organisations within the meaning of the Act unless they are companies incorporated under the *Corporations Act 2001*. The Act does contain an opt-in regime for organisations which are not automatically covered by the Act. Regulations may also be passed requiring specified government/bodies to comply with the Act.
- ◆ **Personal information** – the Act applies only to personal information. Personal information is information or an opinion whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Note that only information about individuals (natural persons) is covered. Information about companies is not regulated by the private sector provisions in the Act.

- ◆ **Privacy Officer** – to facilitate compliance with the privacy regime, the Privacy Commissioner recommends that each organisation should appoint a Privacy Officer. The Privacy Officer is responsible for all matters relating to privacy, particularly in dealing with requests for access to or correction of personal information.
- ◆ **Privacy policy** – NPP 5.1 requires organisations to have a document which provides information in relation to the organisation's approach to privacy. The organisation must give a copy of the document to anyone who asks for it. The matters which must be included in the policy are whether the organisation is bound by the Act or a Privacy Code, where an individual can get more information on the way the organisation manages the personal information it holds, and the fact that an individual can generally obtain access to personal information held. The Privacy Commissioner's Guidelines to the National Privacy Principles suggest various optional items which may be included such as the kinds of personal information held, the purposes for which the information is held and the organisation's contact details.
- ◆ **Sensitive information** - sensitive information is defined in the Act to mean:
  - information or an opinion about an individual's:
  - racial or ethnic origin; or
  - political opinions; or
  - membership of a political association; or
  - religious beliefs or affiliations; or
  - philosophical beliefs; or
  - membership of a professional or a trade association; or
  - membership of a trade union; or
  - sexual preferences or practices; or
  - criminal record, or
  - personal or health information about an individual.

## 2.2 Basic principles

Privacy has emerged as a major business issue in recent years, particularly with the growth of the internet and e-commerce. The privacy regime is an attempt by the Commonwealth Government to address some of those issues. Privacy regulation is founded on the view that privacy is of great importance to individuals and their personal information should be protected and dealt with by organisations in a manner that reflects how the individual concerned would want their information handled.

To comply with the Act, at the time it collects personal information (where practicable) an organisation must disclose:

- ◆ its identity and contact details;

- ◆ what information it collects;
- ◆ for what purposes it collects the information;
- ◆ to whom it discloses the information;
- ◆ that an individual can access the personal information held; and
- ◆ that the organisation is bound by the Act.

There are various qualifications and exceptions to these general principles, and in some cases, positive consent from the affected individual is required, particularly where sensitive information is involved.

The Act also regulates other stages of the collection and use process including data security and transfer of information overseas (see the NPPs summary below for more details).

### **2.3 Guidelines/information circulars**

The Act is administered by the Office of the Commonwealth Privacy Commissioner. The Privacy Commissioner has issued various guidelines and information sheets in relation to the new privacy regime, including the Guidelines to the National Privacy Principles. These Guidelines are non-binding statements of the Privacy Commissioner's views on certain aspects of the new privacy regime and are available on the Privacy Commissioner's website at [www.privacy.gov.au](http://www.privacy.gov.au).

## **3 NPPs SUMMARY**

This section summarises the 10 NPPs and explains how they affect an organisation. It is expressed in the second person to emphasise the importance of individuals within an organisation taking responsibility for privacy compliance.

### **3.1 Collection (NPP1)**

You must not collect personal information unless the information is necessary for one or more of your organisation's functions or activities.

You must ensure that at or before the time of collection, the affected individuals are aware:

- ◆ that their personal information is being collected by your organisation;
- ◆ of your organisation's contact details;
- ◆ that the individuals may obtain access to their personal information; and
- ◆ of the purposes for which the information collected, the organisations to which your organisation usually discloses information and the consequences for the individual if all or part of the information being requested by your organisation is not provided.

### 3.2 Use and Disclosure (NPP2)

Personal information must not be used or disclosed for any secondary purpose unless that purpose is related to the primary purpose of the collection and the individual would reasonably expect the secondary purpose disclosure or the individual has consented.

However, the personal information may be used for the secondary purpose of direct marketing provided that:

- ◆ the information is not sensitive information;
- ◆ there is an opt-out opportunity offered to the individual in all communications with the individual; and
- ◆ your organisation's address and telephone number or some other means by which it can be contacted directly are set out in the communications with the individual.

This is generally known as the direct marketing exception.

Your organisation may also disclose personal information for other specific reasons:

- ◆ to lessen or prevent a serious and imminent threat to a person's life;
- ◆ to lessen or prevent a serious and imminent threat to public health or safety; or
- ◆ if your organisation believes the individual is engaging in unlawful activity and the disclosure is relevant to persons or authorities.

In addition, your organisation may generally disclose personal information it has collected to a related body corporate. However, there are restrictions on transferring personal information to a related body corporate overseas (see the discussion on NPP 9 below). A related body corporate has the meaning given in the *Corporations Act 2001*. It includes a subsidiary and a holding company.

### 3.3 Data quality (NPP3)

You must take reasonable steps to make sure that the personal information your organisation collects, uses or discloses is accurate, complete and up to date.

### 3.4 Data security (NPP4)

Your organisation must take reasonable steps to protect the personal information stored by it from misuse, loss and unauthorised access.

If personal information ceases to be required by your organisation, reasonable steps must be taken to destroy or permanently "de-identify" the information.

### 3.5 Openness (NPP5)

Your organisation must ensure that its policies on the management of personal information are available on request.

It must also take reasonable steps to inform an individual of the personal information it holds in general terms and for what purposes when requested.

### **3.6 Access and correction (NPP6)**

Generally, an individual must be granted access to the personal information relating to them held by your organisation.

You may deny an access request if it is unreasonable or if satisfying the request would reveal evaluative information generated within your organisation in connection with a commercially sensitive decision-making process.

If an individual can show that the personal information held by your organisation is inaccurate, your organisation must take reasonable steps to correct the information.

### **3.7 Identifiers (NPP7)**

Your organisation must not adopt as its own identifier, the identifier or reference of an individual that has already been assigned by an agency (eg tax file numbers or Medicare numbers).

### **3.8 Anonymity (NPP8)**

Where it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with your organisation.

### **3.9 Transborder data flows (NPP9)**

This principle governs the transfer of personal information from within Australia to a place in a foreign country and is based on the restrictions on international transfers of personal information set out by the European Union.

Generally, your organisation will only be able to transfer personal information if it reasonably believes that the recipient of the information is subject to a law that upholds similar principles to the NPPs, and the person has consented to the transfer or the transfer is required to perform a contract with the affected individual.

### **3.10 Sensitive information (NPP10)**

As a general proposition, an organisation must not collect sensitive information about an individual.

But, sensitive information may be collected where the:

- ◆ individual has consented;
- ◆ collection is required or authorised under law; or
- ◆ collection is necessary for research or compilation of statistics relevant to community welfare.

## 4 EXEMPTIONS FROM THE PRIVACY REGIME

### 4.1 General

The NPPs apply to "organisations" and almost all private entities fit within that term. There are some specific exemptions including:

- ◆ small businesses with less than \$3m annual turnover (but see below);
- ◆ media organisations engaged in acts of journalism; and
- ◆ bodies registered under electoral laws and political representatives.

Unless a private sector organisation falls within these exemptions it must comply with the NPPs or equivalent code.

Not all small businesses are exempt. The exemption does not apply to a small business that:

- ◆ is related to another business or entity that is not a small business (including where that other business or entity is based overseas);
- ◆ provides a health service and holds health records;
- ◆ discloses personal information for a benefit, service or advantage;
- ◆ provides someone else with a benefit, service or advantage to collect information; or
- ◆ is a contracted service provider for a Commonwealth contract.

The Act is not intended to affect the use of personal information at a domestic level. Accordingly, the Act provides a broad exemption for the use of personal information in relation to "personal, family or household affairs".

### 4.2 Employee records

In the private sector, the Act does not cover employee records when they are used within the context of an employment relationship for employment related purposes. The exemption includes records relating to both a current and a former employee relationship. It is intended that employee privacy be dealt with under workplace relations legislation at a future time.

An employee's record is basically any record of personal information relating to the employment of an employee. It covers all material from that related to performance or conduct to salary, wage or leave records. It also includes information on such things as trade union membership and sick leave which are also considered sensitive information under the Act.

Note that records relating to potential employees, such as resumés and job applications are not employee records unless the individual concerned actually becomes an employee of the organisation. Accordingly, personal information held on file by your organisation about an unsuccessful job applicant is subject to the Act. The exemption also does not apply to personal information about contractors.

## 5 DIRECT MARKETING

Direct marketing is one of the areas of commercial activity that is most affected by the NPPs and the new privacy regime. Privacy issues must now feature prominently in the planning and conduct of any direct marketing activities.

### 5.1 What is direct marketing?

Direct marketing refers to a range of marketing techniques in which the prospective customer is approached directly via telephone contact, mail or email.

Typically:

- ◆ the contact is unsolicited by the prospective customer; and
- ◆ the prospective customer's details may have come from a variety of sources other than the prospective customer.

Both characteristics place direct marketing right in the "firing line" of the new privacy regime.

Direct marketing includes:

- ◆ telemarketing using names from the telephone book;
- ◆ direct mail to persons whose details are obtained from a commercially available list where the mailout is conducted by your organisation or by a commercial mail house;
- ◆ direct mail to persons whose details are obtained from completing a product warranty card, entering a competition conducted by your organisation or completing a survey conducted by your organisation;
- ◆ telephone contact or mail contact with a person whose name has been provided to you by family or friends; or
- ◆ spam (unsolicited email).

### 5.2 Australian Direct Marketing Association (ADMA)

Your organisation may be a member of ADMA. ADMA has adopted a Code of Practice which includes privacy issues. If your organisation is an ADMA member, it must comply with that Code.

### 5.3 Use must match purpose and collection

The fundamental rule imposed by NPP 2 is that you must only use or disclose personal information for the primary purpose for which you have collected the information.

In some circumstances, direct marketing may actually fall within the primary purpose for which the personal information was collected (see below). The easiest way to achieve this result is to advise the individual of this purpose at the time of collection where information is collected directly from the individual.

In many circumstances, however, your organisation's direct marketing activities will represent a secondary use of the information. For a secondary purpose use to be lawful, it must fall within one of the following exceptions to the primary purpose general rule:

- ◆ where the secondary purpose is related to the primary purpose of collection (for sensitive information, the secondary purpose must be directly related to the primary purpose of collection);

and

the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

- ◆ where the individual has consented to the particular use; or
- ◆ the specific, but limited, exemption granted to direct marketing.

#### **5.4 Primary purpose**

Where you have collected the personal information directly from the individual to whom it relates, the primary purpose is likely to be clear to you (and to the individual). The individual is very likely to have provided the information for a particular purpose which will be the primary purpose. The information may be used for the primary purpose without relying on any exceptions.

#### **5.5 The direct marketing exception**

The direct marketing exception operates to protect an organisation in its initial contact with an individual in some situations (and subsequent contacts provided certain conditions are satisfied).

The exception applies to direct marketing where:

- ◆ obtaining the individual's consent is impracticable; and
- ◆ the individual is told in each direct marketing communication they can opt out of receiving any further marketing from the organisation.

Once you have made the initial contact based on this exception, for each subsequent communication the individual's failure to opt out is taken to be their implied consent.

Each communication (including the initial contact) with the individual should identify your organisation and give the individual the opportunity to decline any further material. Although an opt-out opportunity is strictly only required where you do not have prior consent or have given notification, we recommend including an opt-out in all direct marketing material. If the communication is written, it must also include your organisation's:

- ◆ ACN and business address;
- ◆ telephone number; and

- ◆ if by fax, telex or email, a number or address at which your organisation can be contacted.

**(a) Non-sensitive information**

Note that the direct marketing exception does not apply to sensitive information. It applies to non-sensitive personal information only. In other words, you cannot rely on the direct marketing exception to use sensitive information for direct marketing purposes.

**(b) Use but do not disclose**

The second point to note is that the exception is limited to the use of the personal information by the organisation relying on the exception. It does not permit the disclosure of personal information to another entity for direct marketing purposes.

**(c) Impracticable to obtain consent**

The exception only applies where it is impracticable to obtain consent. Do not confuse "impracticable" with "inconvenient". If you are in regular contact with the individual on any matters, obtaining their consent is not likely to be impracticable.

Where you have such contact or contact is relatively inexpensive, for example email contact, it is unlikely that your organisation will be able to rely on this exception.

As you would perhaps expect, another significant factor will be the particular consequences for the individual of receiving the direct marketing information without consent.

**(d) Opting out**

The opt out must be clear to the individual, readily accessible and at no significant cost to the individual.

## **6 DEALING WITH ACCESS AND CORRECTION REQUESTS**

The Act gives individuals a right to have access to personal information an organisation holds about them (with some exceptions). When dealing with a request by an individual for access to their personal information consider the following issues:

- ◆ take reasonable steps to establish the identity of the person making the request;
- ◆ find out what information the individual wants. Do they want all the personal information you hold, or just some parts?
- ◆ the Privacy Commissioner's Guidelines suggest that a written request for access should be acknowledged as soon as possible and within 14 days at the latest. The Guidelines also suggest that access should be granted within 14 days for straightforward requests and 30 days for more complicated requests;
- ◆ there is no prescribed fashion for providing access. Accordingly, access should be provided in a fashion which is:

- consistent with the form of the request; and
- appropriate and practical, given the nature of the information sought and the special needs or disabilities of the applicant;
- ◆ in general terms, organisations may refuse a request for access to personal information in a variety of circumstances, including situations where:
  - providing access would pose a serious and imminent threat to the life or health of a person;
  - providing access would unreasonably impact on the privacy of others;
  - the request is frivolous or vexatious;
  - there are legal proceedings between the parties (actual or anticipated) and access to the information would not be available as part of the discovery process – consult lawyers if you have any doubts;
  - providing access would prejudice negotiations between the organisation and the individual by showing the organisation's intentions;
  - the law prohibits or authorises denial of access or giving access would be likely to prejudice law enforcement activities; or
  - providing access would give access to a commercially sensitive decision making process;
- ◆ before refusing access entirely, consider alternatives that may meet the needs of the individual concerned, such as:
  - blocking out the information covered by the exception;
  - giving a summary of the information, excluding the information covered by the exception; or
  - using an intermediary (as discussed below);
- ◆ under NPP 6.4, an organisation may charge for accessing information, as long as that charge is not excessive. The Privacy Commissioner has interpreted this to mean that an organisation will generally be entitled to recover its costs in providing the information;
- ◆ NPP 6.3 requires that an organisation consider using an independent third party (an intermediary) to assist in giving an individual access to information that would otherwise be excluded under NPP 6.1;
- ◆ under NPP 6.5, if an individual can establish that the personal information you hold about them is inaccurate, out of date or incomplete, you must take reasonable steps to correct that information;
- ◆ if you disagree with an individual over the accuracy of their personal information you may refuse to amend it. However, you must make a note with the information in question that the individual disputes its accuracy;

- ◆ you must give reasons if you refuse access to, or refuse to correct, personal information.

## **7 OTHER THINGS THE ACT COVERS**

In addition to the NPPs, the Act includes a set of 11 IPPs which set out the privacy requirements that Commonwealth Government departments and agencies must comply with when handling personal information. The IPPs contain similar, but different, obligations to the NPPs regarding how personal information is collected, stored, used and disclosed by government agencies.

Part IIIA of the Act contains privacy principles for dealing with personal information for consumer credit reporting. This legislation is supplemented by the Credit Reporting Code of Conduct issued by the Privacy Commissioner.

Together they set out requirements for dealing with requests by individuals for access to their credit information, accuracy and type of information collected, disclosures of credit information and settling of credit reporting disputes.

## **8 OTHER LAWS RELEVANT TO PRIVACY**

Privacy obligations can also be found outside the Act. Specific privacy requirements are set out in several other areas of law, including:

- ◆ Crimes Act 1914 (Cth) which deals with disclosures of information regarding quashed (ie set aside), pardoned or spent (ie minor convictions more than 10 years ago) convictions.
- ◆ Freedom of Information Act 1982 (Cth) which provides a general right of access to information held by the Commonwealth Government and similar State legislation.
- ◆ Taxation Administration Act 1953 (Cth) which, combined with the Act places strict limits on the collection and use of tax file numbers for identification purposes.
- ◆ Telecommunications Act 1997 (Cth) which originally placed specific obligations on companies involved in the telecommunications sector when handling customers' personal information. Many of these obligations have now been reflected in the NPPs.
- ◆ Certain States also have privacy legislation in place, largely directed at governmental entities.

## **9 CONSEQUENCES**

The Act establishes a complaints mechanism that can be accessed by any individual who believes there has been an interference with their privacy. The individual can complain to the Privacy Commissioner. In the first instance, the complaint is referred back to the organisation against which the complaint has been made. If the complaint is not resolved by the organisation and the individual, the Commissioner will get involved and may make a formal determination either dismissing or

substantiating the complaint. The Commissioner may in fact investigate potential breaches of the Act without first receiving a complaint from an individual.

An individual or the Privacy Commissioner can, if necessary, seek to have a determination by the Privacy Commissioner enforced by the Federal Court. If the Court is satisfied that the respondent has engaged in conduct that constitutes an interference with the complainant's privacy, the Court may make such orders as it thinks fit. This is a broad power which allows the Court to, eg:

- ◆ order damages;
- ◆ grant an injunction (eg restraining your organisation from further use of a particular database or marketing technique until the issue is settled by the Court);
- ◆ make an order tailored to the particular circumstances (eg requiring your organisation to remove entries from a database); or
- ◆ make declarations as to the parties' rights. Dealing with a complaint takes time and diverts valuable organisational resources. Significant adverse publicity may also result from a privacy complaint.

## 10 PRIVACY SCENARIOS

### 10.1 Scenarios

This section considers the privacy implications of the scenarios below by discussing the general principles and then applying them (principle by principle) to the following scenarios:

- ◆ Your organisation is contacted by someone wanting further information about a product or service you offer.
- ◆ Name, address and credit card details are provided during a product purchase.
- ◆ Business cards are exchanged at a function.
- ◆ A customer completes a tear off part of a product brochure offering further information on a product.
- ◆ Your organisation employs a telemarketer to conduct general market research using public telephone directories.

### 10.2 Collection

As the collector of personal information you have certain responsibilities. NPP 1 contains various rules on the collection of personal information set out above.

You should consider:

- ◆ **Necessity for information** - is the collection of the personal information necessary for the performance of your organisation's functions and activities? There must be a particular purpose in mind when the information is collected.

- ◆ That purpose may be the collection of the information on behalf of another party, if that collection is a function of the organisation. You cannot collect information simply because it may be useful in the future.
- ◆ **Identity and access** - have you notified the individuals from whom you collected the personal information as soon as practicable of the matters listed in NPP 1.3 including:
  - our organisation's identity;
  - the fact that the person is able to gain access to the information; and
  - the purposes for which the personal information is being collected by your organisation.
- ◆ **Disclosures** - have you notified the individual about the organisations to which you usually disclose information of that kind? This does not mean you must name the individual organisations. They may be referred to by category, for example, licensing organisations, mailing houses, internet service provider etc.
- ◆ **Legal requirements** – have you notified the individual about any law that requires you to collect personal information?

In each of the scenarios, NPP 1.1 requires that your organisation only collects information that is necessary to perform the particular function. In some circumstances a minimum amount of information may be all that is required. For example, if you receive an email request via your website for information, on a strict interpretation, it may only be necessary to obtain the individual's email address to provide the information they have requested. It is expected, however, that the Privacy Commissioner will take a pragmatic approach when determining what information is necessary and will consider what information is normally exchanged in a commercial environment.

Relevant examples include:

- ◆ Your organisation is contacted by someone wanting further information about a product or service you offer – *the only necessary information would be the address (postal or email) to which the information is to be sent, although it would be reasonable to collect a name and contact details in case of any difficulty with providing the information.*
- ◆ Name, address and credit card details are provided during a product purchase - *no further information would ordinarily be necessary other than details of the product purchased.*
- ◆ Business cards are exchanged at a function – *sufficient information would be contained in the business card.*
- ◆ A customer completes a tear off part of a product brochure offering further information on a product – *the only necessary information would be details required to deliver the information requested as well as details of the information supplied.*
- ◆ Your organisation employs a telemarketer to conduct general market research using public telephone directories – *in most situations it would not be necessary to identify the individual being questioned, except perhaps for*

*quality assurance purposes. In some circumstances you may request a name if you will be contacting them again, or other details if the individual is entitled to a "gift" or competition entry for taking part.*

### 10.3 Use

The general rule established by NPP 2 is that personal information can only be used for the primary purpose for which it was collected. Generally, any use should be directly related to that purpose. Other uses are permitted where:

- ◆ **related purpose** - the secondary use is related to the primary purpose for which the information was collected (directly related if the information is sensitive information) and the individual would reasonably expect you to use the information for that purpose; or
- ◆ **consent** - the individual has consented to the use.
- ◆ Your organisation is contacted by someone wanting further information about a product or service you offer – *the primary use for the information collected would be to provide the individual with the information they have requested.*
- ◆ Name, address and credit card details are provided during a product purchase – *obviously the primary purpose for collecting this information would be to charge the individual's credit card account for the purchase. There is unlikely to be any other permitted use.*
- ◆ Business cards are exchanged at a function - *using a person's contact details taken from a business card to send them a Christmas card would be a permissible secondary use of the information.*
- ◆ A customer completes a tear off part of a product brochure offering further information on a product – *again, the primary use for the information collected would be to provide the individual with the information they have requested. Use of this information to provide the person with details of a new replacement product would be a permissible secondary use of the information, but use of the information to provide the person with details of other products would not fall within the permitted secondary purpose but could be allowed by the direct marketing exception.*
- ◆ Your organisation employs a telemarketer to conduct general market research using public telephone directories – *market research and related uses, such as product development, would be the primary use for the information collected. Other uses, such as direct marketing would only be permissible if the criteria for the direct marketing exception (as discussed above) are met.*

### 10.4 Disclosure

NPP 2 sets out the fundamental rule that you must not disclose personal information for a purpose other than the primary purpose of collection. Most of the obligations imposed by the NPPs on the use of personal information also apply to disclosure of personal information.

The general rule means that if you did not collect the information for the primary and notified purpose of transferring it to another organisation, your organisation can only use or disclose it for that purpose if the transfer can fit within the above exceptions.

The organisation receiving the personal information from your organisation may have the same obligations. Depending on your relationship with the recipient organisation, it may be simpler for you to simultaneously provide the individual with this information for both your organisation and the recipient organisation. If not, the recipient organisation must provide this information to the individual as soon as practicable.

Some relevant examples include:

- ◆ Your organisation is contacted by someone wanting further information about a product or service you offer - *if the information will be delivered to the individual concerned by courier, then disclosing their address details would be a permitted disclosure as it would be reasonably expected by the individual.*
- ◆ Name, address and credit card details are provided during a product purchase – *providing the information to the credit card company would be a permitted disclosure. Any other disclosure is unlikely to be permitted.*
- ◆ Business cards are exchanged at a function - *it may be permissible to pass the details of the individual concerned on to a colleague looking for a particular service which the individual is able to provide as that could be considered a reasonably expected use of a business card.*
- ◆ A customer completes a tear off part of a product brochure offering further information on a product – *if the information will be delivered to the individual concerned by courier, then disclosing their address details would be a permitted disclosure as it would be reasonably expected by the individual.*
- ◆ Your organisation employs a telemarketer to conduct general market research using public telephone directories – *if information is collected anonymously, it will be able to be disclosed for any purpose. However, if survey results are linked with identifying information, you will need the individual's permission to disclose it to others, such as a promotions company.*

## 11 CHECKLIST

There are many requirements in the Act, often with exceptions and qualifications. Here is a big picture checklist covering the regime applying to the private sector as contained in the NPPs:

- ◆ only collect the personal information you need;
- ◆ ensure you tell people what information you are collecting, why you are collecting it and to whom you may disclose it;
- ◆ only use or disclose personal information for the purpose it was collected;
- ◆ consider the privacy implications of direct marketing activities;
- ◆ ensure the personal information your organisation holds is accurate and up to date;
- ◆ de-identify personal information you no longer need;
- ◆ ensure personal information is stored securely;

- ◆ ensure your organisation's information handling practices are known and that you have a privacy policy;
- ◆ allow people to check the information that your organisation holds about them and if the information is not correct, change it;
- ◆ do not adopt governmental identifiers such as tax file numbers to identify your customers and business partners;
- ◆ allow people to deal with your organisation without identifying themselves where possible;
- ◆ do not transfer personal information overseas unless the recipient is subject to privacy laws or requirements at least as stringent as the NPPs;

and

- ◆ do not collect sensitive information without the individual's consent.