

Privacy Policy

Meertens

March 2022



Introduction

In December 2000, Federal parliament passed the Privacy Amendment (Private Sector) Act 2000. The ensuing information reflects the firms procedures for handling personal information by adopting the National Privacy Principles (NPP's). A complaint handling procedure has been set up to deal with any issues that arise.

Policy Statement

Meertens acknowledges the importance of adhering to the NPP's and the requirements of the Privacy Amendment (Private Sector) Act 2000. We undertake to treat all client and other personal information in our possession in accordance with the requirements of the Act.

Definitions

The definitions are instrumental to understanding the Act. So as to minimise any possible misunderstandings these have been taken directly from the documentation provided by the Privacy Commission.

Personal Information: Is information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It includes all personal information regardless of its source. Personal information relates to a natural living person. A natural person is a human being rather than, for example, a company, which may in some circumstances be recognised as a legal 'person' under the law.

Sensitive Information: Is a subset of personal information. It means information or opinion about an individuals 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 preferences or practices, criminal record or health information about an individual.

Collection: An organisation collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when an organisation keeps personal information it has come across by accident or has not asked for.

Consent: Means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. Consent is invalid if there is extreme pressure or coercion.

The National Privacy Principles

The ten NPP's will be addressed as follows:

1. Collection:

Personal Information will not be collected unless it is necessary for one or more of the firms functions or activities. The collection will be fair, lawful and not intrusive. A person will be told the organisations name, the purpose of the collection, that the person can get access to their information and what happens if the person does not give the information.

2. Use and Disclosure:

We will only disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances related to public interest such as law enforcement and public or individual health and safety.

3. Data Quality:

A review of personal information will be made every 12 months to ensure that the information we collect, use or disclose is accurate, complete and up to date.

4. Data Security:

We have taken reasonable steps to protect the personal information we hold from misuse and loss and from unauthorised access modification or disclosure. Staff are required to sign a confidentiality clause as part of their contracts of employment.

Training is provided to staff in relation to the privacy act and a 12 month privacy audit cycle has been put in place.

Technology – there is extensive technology-based security through a secure network environment.

Physical Security – is maintained through controlled keys for staff to access the office environment.

Physical information – is destroyed by means of secure shredding.

Electronic information – is destroyed by deleting it from the network.

5. Openness:

This policy document clearly expresses our policy on managing personal information. A copy of this policy is available at no cost upon request.

6. Access and Correction:

We will provide access to personal information upon request. The only exceptions are as noted in 6.1(a) to (k) of the legislation. If it is established that the information is not accurate, complete and up-to-date, we will take reasonable steps to ensure that the situation is rectified.

7. Identifiers:

We do not adopt, use or disclose any identifiers that have been assigned by a Commonwealth Government Agency.

8. Anonymity:

Although unlikely given the nature of our business, we will give people the option to interact anonymously whenever it is lawful and practicable to do so.

9. Transborder Flows of Data:

We will only transfer personal information to a recipient in a foreign country where the information will have appropriate protection or where consent has been obtained.

10. Sensitive Information:

We will not collect sensitive information unless the individual has consented, it is required by law – or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety.

When do the NPP's apply?

The ten NPP's will be addressed as follows:

NPP	Topic	What information the NPP applies to
NPP 1	Collection	Only applies to information collected after 21 December 2001
NPP 2	Use and Disclosure	Only applies to information collected after 21 December 2001
NPP 3	Data Quality and Collection	As it applies to collection only applies to information collected after 21 December 2001
NPP 3	Data Quality on Use and Disclosure	As it applies to use and disclosure it applies regardless of when it was collected
NPP 4	Data Security	Applies regardless of when it was collected
NPP 5	Privacy Policies and Openness	Applies regardless of when it was collected
NPP 6	Access and Correction	If information already held is not used or disclosed, it only applies to information collected after 21 December 2001 but if information already held is used or disclosed after commencement then rights of access and correction apply unless: <ul style="list-style-type: none"> • Unreasonable administrative burden, or • Cause the organisation unreasonable expense
NPP 7	Commonwealth Government Identifiers	Applies regardless of when it was collected
NPP 8	Anonymity	Only applies to information collected after 21 December 2001
NPP 9	Transborder Data Flow	Applies regardless of when it was collected
NPP 10	Collection of Sensitive Information	Only applies to information collected after 21 December 2001

Enquiries and Complaints Handling Procedure

The firm has appointed Austin Taylor as the staff member who is responsible for privacy within the firm as it relates to the act (“the Privacy Officer”).

It is possible that a client, or prospective client, might require a copy of our Privacy Policy (Refer NPP5 – Privacy Policies and Openness). All enquiries are to be directed to the Privacy Officer.

It is imperative that the Privacy Officer be made aware of any complaints that are made.

Any staff member who has concerns as to how information is being dealt with is to raise the issue initially with a Director and then with the Privacy Officer. Should there be a fault with the procedures, all reasonable steps will be taken to ensure that it is rectified as soon as practicable.

If a client makes a complaint it will be dealt with in the following manner:

- Initially a Director will be made aware of the complaint. In the first instance they will make every effort to resolve the issue.
- If the Director cannot immediately resolve the issue, then it will be escalated to the Privacy Officer. The matter will be fully investigated whether it is client or staff initiated to ensure compliance with the Act. A response will be conveyed to the complainant within 30 days.

Should there be any procedure or procedures which is or are causing a breach of the Act, then they will be rectified immediately following the investigation.

Exemptions

Employee Records are exempt from the operation of the Act if the organisation is or has been an employer of the individual in question and the act or practice is directly related:

- To a current or former employment relationship between the employer and the individual, and
- To an employee record held by the organisation

This exemption does not apply to prospective employees.