

Privacy Policy

Trinity Law ('the Firm') is subject to the *Privacy Act 1988* ('the Act'). The Act regulates how the Firm collects, uses, stores and discloses Personal Informationⁱ. In this regard, the Firm is committed to protecting the privacy of its clients, maintaining the confidentiality of their Personal Information and applying the Australian Privacy Principles ('APP').

The Firm subscribes to the following Privacy Policy:

1. Personal and Sensitive Information

The Firm will collect Personal Information and sometimes Sensitive Informationⁱⁱ e.g. financial records, tax file numbers and medical records, about its clients in order to provide legal services. The Firm is committed to only collecting Personal Information which is necessary for the provision of legal services and the operation of the Firm.

The provision of Personal Information by our clients is optional. However the Firm's ability to provide legal services may be limited should the client choose not to provide the required Personal Information. If that occurs, the Firm may end its retainer.

2. Collection

The Firm will only collect Personal Information by lawful and fair means, and which is relevant to the scope of legal services required. If the need arises, further Personal Information may need to be collected from the client in the future. The Firm will not collect Personal Information unless the information is reasonably necessary for the Firm to conduct the client's matter.

When the Firm collects Personal Information about an individual, the Firm will take reasonable steps at or before the time of collection to ensure that the individual is aware of certain key matters, such as:

- a. the identity of the Firm;
- b. the fact that the information has been collected;
- c. whether the information was required under an Australian law, or court/tribunal order, and the details of the law, court of tribunal, the purposes for which information is collected;
- d. the main consequences (if any) of not collecting the information;
- e. the organisations (or types of organisations) to which the Firm would normally disclose information of that kind;
- f. the fact that the individual is able to access the information;
- g. how to complain about a breach of an APP; and
- h. whether the information is likely to be disclosed to overseas recipients.

3. Sensitive Information

The Firm will not collect Sensitive Information unless:

- a. the information is reasonably necessary for the Firm to conduct the matter or;
- b. the collection of the information is required or authorised by or under an Australian law or a court/tribunal order;
- c. a Permitted General Situationⁱⁱⁱ exists in relation to the collection of the information by the Firm; or
- d. a Permitted Health Situation^{iv} exists in relation to the collection of the information by the Firm.

4. Disclosure by the Firm

Clients agree the Firm can disclose Personal Information to a third party e.g. other lawyers, accountants, banks, witnesses, and government agencies if it is required as part of the Firm

providing legal services. The client will, if it requests the Firm in writing, be provided with details of the recipient. The Firm will use its best efforts to provide legal services without the need to disclose Personal Information and will obtain consent from the client should the need for disclosure other than in the ordinary course of the provision of legal services arise, except where the information must be provided by the Firm under:

- a. an Australian law; or
- b. a court/tribunal order; or
- c. other legal obligations.

5. Disclosure for a secondary purpose

The Firm will not use or disclose Personal Information for a secondary purpose unless

- a. it has obtained consent to do so,
- b. the individual would reasonably expect the Firm to use or disclose the information for the secondary purpose which is directly related to the primary purpose;
- c. it is required or authorised under an Australian law or court/tribunal order;
- d. a Permitted General Situation exists;
- e. a Permitted Health Situation exists; or
- f. the Firm believes it reasonably necessary for one or more enforcement activities by, or on behalf of an enforcement body.

Where the firm has used or disclosed information under b – f above, the Firm will take steps as are reasonable to ensure the information is de-identified before being used or disclosed

6. Transfer of Personal Information overseas

If the Firm is required to transfer any Personal Information outside Australia, the Firm will comply with the provisions of the Act which apply to cross border data flows. The Firm will only transfer Personal Information overseas where the context of the matter requires it. The Firm will first take reasonable steps to ensure the recipient does not breach the APPs in relation to the information, except where:

- a. the Firm believes the recipient is subject to a scheme offering the same protection as the Australian Privacy Principles, and there are mechanisms for the individual to enforce that protection;
- b. after being told that if the individual consents to the disclosure, the Firm is not required to ensure that the recipient conforms to the APP, and the individual consents regardless;
- c. the disclosure is required or authorised under an Australian law or court/tribunal order; or
- d. a Permitted General Situation (other than the situation referred to in item (g) or (h) of the definition of Permitted General Situation below) exists in relation to the disclosure of the information by the Firm.

7. Identification

Where possible, and if directed by an individual, the individual will not be required to identify themselves when dealing with the Firm in relation to a particular matter. The individual will be required to identify themselves however where:

- (a) the Firm is required or authorised under an Australian law or a court/tribunal order to deal only with individuals who have identified themselves; or
- (b) it is impractical for the Firm to deal with individuals who have not identified themselves.

Generally, an individual will be required to identify themselves when they are a client of the Firm. However, the Firm will not disclose a client's identity to a third party unless the matter

necessitates it, or as directed by the client. The Firm will not adopt a government related identifier of an individual (including those assigned by a state or territory) as its own.

8. Unsolicited Personal Information

If the Firm receives unsolicited Personal Information, the Firm will determine as soon as possible, whether the information is required for the client's purposes with the Firm. If the information is not required, provided it is lawful and reasonable to do so, the Firm will either destroy the information, or ensure that it is made known to the individual.

9. Security

The Firm will use all prudent methods to keep all Personal Information safe and secure from unauthorised access through the use of firewalls, anti-virus software and secure filing systems. Where the Personal Information is no longer required for the purpose for which it was disclosed, and the Firm is not required by law to retain it, the Firm will take reasonable steps to destroy the information.

10. Access to Personal Information

Clients are entitled to access their Personal Information held by the Firm, provided that one of the following exceptions does not apply:

- a. the Firm reasonably believes that giving access would pose a serious threat to the life, health or safety of an individual, or to public safety;
- b. giving access would in the Firm's opinion, have an unreasonable impact on the privacy of other individuals;
- c. the request for access is frivolous or vexatious;
- d. the information relates to existing or anticipated legal proceedings between the Firm and the client, and would not be accessible through the process of discovery in those proceedings;
- e. giving access would reveal the intentions of the Firm in relation to negotiations with the client in such a way as to prejudice those negotiations;
- f. giving access would be unlawful;
- g. denying access is required or authorised by or under an Australian law or a court/tribunal order;
- h. both of the following apply:
 - i. the Firm has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Firm's functions or activities has been, is being or may be engaged in;
 - ii. giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- i. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- j. giving access would reveal evaluative information generated within the Firm in connection with a commercially sensitive decision making process.

Upon request by a client for access to Personal Information, the Firm will respond and provide access within a reasonable time, if it is reasonable and practical to do so.

If the Firm refuses to give the client access to the Personal Information for a reason detailed above, the Firm must:

- a. endeavour to take reasonable steps to give access in a way that meets the needs of the Firm and the client; or
- b. provide a written notice to the client that sets out:

- i. the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so;
- ii. the mechanisms available to complain about the refusal; and
- iii. any other matter prescribed by the regulations to the Act.

The Firm may charge a reasonable fee to the client for costs incurred in providing the information to the client.

11. Information integrity

The Firm wishes to maintain the integrity of the Personal Information that it holds by updating its databases as required. Clients are encouraged to notify the Firm immediately if there is a change to their Personal Information by contacting the Firm's Privacy Officer on (02) 6163 5050.

If the Firm is satisfied that Personal Information about a client held by the Firm, having regard to the reason the Personal Information is held, is inaccurate, out of date, incomplete, irrelevant or misleading, or the client requests the Firm to update or correct the Personal Information, then the Firm will take all reasonable steps to correct the information. The client may request that the Firm update the Personal Information provided by the Firm to any other entity on behalf of the client.

Even if requested to do so, the Firm may refuse to correct Personal Information, in which case the Firm will give the client a written notice setting out:

- i. the reasons for the refusal to correct the Personal Information (except where it would be unreasonable to provide those reasons);
- ii. mechanisms available to the client to complain about the refusal; and
- iii. any other matter prescribed by regulation.

Where the Firm has refused to correct the Personal Information of a client, the client may request that the Firm associate a statement with the Personal Information that the Personal Information is inaccurate, out of date, incomplete, irrelevant or misleading. The statement will be made apparent to users of the Personal Information.

Where a request is made by a client to update or attach a statement to the information, the Firm will respond within a reasonable period after the request is made.

12. Credit card information

Credit card information may be obtained for payment processing only. Credit card information is not stored on the Firm's database, however receipts will be kept on file or with our accounts department.

13. Names and addresses

The Firm values its clients greatly. It does keep a record of clients' names and addresses for ensuring that there is no conflict in acting for one client against another. The Firm also uses this list for its own marketing and distribution of material, and as a client, unless you tell us, the Firm assumes you agree to receive material from us. However, this information is not and will not be divulged outside the Firm, and a client can, of course, at any time, request to be removed from any list or mail or email material, and the Firm will happily do so.

14. Retention

The Firm is legally required to maintain files for a period of 7 years following completion of a matter. All files are held in a safe and secure location with limited access. After 7 years all files including Personal Information, will be destroyed.

15. Errors

The Firm will promptly correct any error about a client's Personal Information as soon as it is brought to the Firm's attention. Information on accessing Personal Information records may be obtained by contacting the Firm's Privacy Officer on (02) 6163 5050.

16. Complaints

Clients may contact the Firm's Privacy Officer on (02) 6163 5050 if a client has any concerns or complaints about the manner in which Personal Information has been collected or handled by the Firm.

ⁱ **Personal Information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

ⁱⁱ **Sensitive Information** means

(a) information or an opinion about an individual's:

- i. racial or ethnic origin; or
- ii. political opinions; or
- iii. membership of a political association; or
- iv. religious beliefs or affiliations; or
- v. philosophical beliefs; or
- vi. membership of a professional or trade association; or
- vii. membership of a trade union; or
- viii. sexual orientation or practices; or
- ix. criminal record;

that is also Personal Information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

ⁱⁱⁱ **Permitted General Situation** means

a. it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and

b. the Firm reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety,

OR

c. the Firm has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Firm's functions or activities has been, is being or may be engaged in; and

d. the Firm reasonably believes that the collection, use or disclosure is necessary in order for the Firm to take appropriate action in relation to the matter,

OR

e. the Firm reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and

f. the collection, use or disclosure complies with the rules made under subsection (2),

OR

g. the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim,

OR

h. the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

^{iv} **Permitted Health Situation** means a situation described in paragraph 16B of the APPs.