VETERANS COMPENSATION ASSOCIATION
JUSTICE FOR THOSE WHO SERVED

Privacy policy

Privacy Act

Our business is bound by the Privacy Act 1988 (the Act) and the Australian Privacy Principles (APP). Our business is an APP entity as defined in s 6(1) of the Act.

We collect and hold personal information relating to our clients and to other people and entities associated with our clients as may be provided or disclosed to us in the course of business. Such personal information may include, but is not limited to, names, tax file numbers, addresses, telephone numbers, social media details, email addresses, occupations, wage records, bank account details, asset and investment details, financial planning records, taxation records, medical records and relationship details.

Personal information is collected from our clients in the following ways:

- by providing it to us directly;
- by authorising third parties to provide it to us;
- by other parties providing it to us either voluntarily or pursuant to compulsory processes we conduct on our client's behalf.

How is personal information received and held?

Personal information may be received and held either as a hard copy, paper, or a soft copy being electronic data, in any available form. In either case, we take the security of personal information very seriously. We secure hard copy documents carefully in and out of our office. We use cyber-security systems to protect soft copy documents. We never ask for bank details or other sensitive information by email.

For what purpose is personal information collected, held, used and disclosed?

All data is processed by the business on a lawful basis. The purposes for which we collect, hold, use and disclose personal information are:

- to offer our products and services to our clients. In doing so we may disclose personal information to other people or entities involved in the provision of the product or service,

such as government departments and individuals. Unless compelled by law, we will never disclose personal information without the client's knowledge and consent;

- to facilitate our internal and external administrative processes including financial and business operations and reporting requirements;
- to obtain, maintain and comply with the terms of our professional indemnity and other insurance policies; and
- to comply with applicable laws.

How can personal information be accessed or corrected?

Clients may access their personal information and seek correction of it at any time by applying to our office in person or in writing.

Clients will be formally identified before releasing or amending any personal information.

Is personal information disclosed outside of Australia?

Where necessary we will disclose personal information to overseas recipients, including a related body corporate. The likely countries that information might be sent to include [Insert locations].

What is the complaints process relating to personal information?

If there is a breach of this privacy policy, either of the Act or the Australian Privacy Principles (APP), a complaint may be made by the client to:

- our customer services team; or
- the Office of the Australian Privacy Commissioner.

Data breaches

All staff are responsible for protecting the confidentiality of client information and business information. Refer any data breaches, or suspected data breaches, to the customer services team as soon as possible.

What is an eligible data breach?

An eligible data breach, defined in s 26WE(2) of the Act, is when:

(a) both of the following conditions are satisfied:
- *(i) there is unauthorised access to, or unauthorised disclosure of, the information;*
- *(ii) a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or*

(b) the information is lost in circumstances where:
- *(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and*
- *(ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates;…*

If there is a suspicion of a breach

If we suspect that there has been an eligible data breach, a reasonable and expeditious assessment will be conducted within 30 days.

If we believe or have reasonable grounds to believe there has been a breach then a statement will be prepared setting out:

- the business's details;
- a description of the breach;
- the kind or kinds of information concerned; and
- recommendations about the steps that we will take in response to it.

If practicable, we will advise the contents of the statement to each of the affected clients who may be at risk from the breach. If this is not practicable we will publish the statement on our website and take other reasonable steps to publicise its contents. Communications with individuals will be via their preferred communication method.

The statement will be submitted to the Privacy Commissioner.

Exception to reporting

Mandatory notification requirements are waived if remedial action can be taken that results in a reasonable person concluding that the access or disclosure is not likely to result in serious harm to any of those individuals.