

WBP Group Privacy Policy

WBP GROUP AUSTRALIAN PRIVACY PRINCIPLES (APP) PRIVACY POLICY

EFFECTIVE DATE: 22ND FEBRUARY 2018

POLICY OVERVIEW

WBP Group and its related entities recognise the importance of protecting privacy and are committed to compliance with the Privacy Act 1988^{Ch} (**Privacy Act**). This policy has been adopted as a part of our commitment. This document sets out how WBP Group and any related entities will handle personal information, including an overview of the types of personal information generally retained, and how personal information is collected, used, disclosed and stored. This document also sets out WBP Groups commitment to notification requirements under the Privacy Amendment Act 2017 (the NDB scheme).

WHAT PERSONAL INFORMATION IS COLLECTED

WBP Group may collect or otherwise retain personal information during the ordinary course of conducting Valuation, Advisory or any other business.

Personal information is defined in the Privacy Act as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable':

- a) whether the information or opinion is true or not, and
- b) whether the information or opinion is recorded in a material form or not (s 6(1)).

Generally, the types of personal information collected or otherwise retained by WBP Group may include but is not necessarily limited to:

- a) Name; and
- b) contact details including but not necessarily limited to:

WBP Group Privacy Policy

- i. email address;*
 - ii. postal address;*
 - iii. residential address; and*
 - iv. home, mobile, and or business telephone numbers*
- c) Any other information which may be located within documentation provided to WBP Group or otherwise obtained and retained on file which may include but is not limited to documents such as:
 - i. contracts of Sale;*
 - ii. Certificates of Title (and any associated documents);*
 - iii. planning, building or any other project documentation; and*
 - iv. any other documentation retained on file as a part of conducting business.*

SENSITIVE INFORMATION

Sensitive information is defined in the Privacy Act to include information or opinions about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information. It is our commitment that sensitive information will be used only:

- a) for the primary purpose for which it was obtained;
- b) for a secondary purpose that is directly related to the primary purpose;
- c) with your consent; and/or
- d) where required or authorised by law

HOW IS INFORMATION COLLECTED

Personal information may be collected or otherwise retained through various means, either directly or from third parties. This may include:

Directly, when a party:

- a) provides information to WBP Group at the point of instruction;
- b) participates in any applicable email subscription;

WBP Group Privacy Policy

- c) completes any online form
- d) participates in a subscription;
- e) sends WBP Group an email or written correspondence;
- f) lodges a complaint
- g) submits a job application
- h) makes payment
- i) registers for an event
- j) calls WBP Group

By third parties:

- a) as a part of instructions provided to WBP Group;
- b) as obtained during the course of conducting ordinary business in accordance with industry requirements or industry best practice and/or company requirements.

HOW IS INFORMATION USED OR DISCLOSED

Generally, when WBP Group receives personal information it is in relation to, or provided together with, other information that is in connection with WBP Group's business activities. At the broadest level, WBP Group therefore collects personal information for the primary purpose of conducting activities as may be required during the course of conducting business. We generally use and disclose personal information for the purposes for which we collect that personal information and any directly related purpose, or if required by law, industry requirements or industry best practice. This includes disclosing personal information to service providers who assist us in our functions and activities only when reasonably necessary to assist in those functions and activities.

WBP Group may use personal information:

- a) as may be required during the course of completing any activities related to Valuations, Advisory or any other services;
- b) as may be required in order to ensure that WBP Group retain prudent file records in accordance with industry requirements and/or best practise;
- c) as may be required to assist with the administration of WBP Groups operations;

WBP Group Privacy Policy

- d) as may be required when providing valuation reports or other services as instructed by third parties;
- e) with companies acting as our authorised agents in providing our service;
- f) when legally compelled to do so

It is not considered likely that WBP Group will disclose information to overseas recipients.

Direct Marketing

WBP Group may use personal information other than sensitive information for marketing purposes if:

- a) the organisation collected the information from the individual; and
- b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and
- c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
- d) the individual has not made such a request to the organisation.

WBP Group may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- a) WBP Group collected the information from:
 - i. *the individual and the individual would not reasonably expect the WBP Group to use or disclose the information for that purpose; or*
 - ii. *someone other than the individual; and*
- b) either:
 - i. *the individual has consented to the use or disclosure of the information for that purpose; or*
 - ii. *it is impracticable to obtain that consent; and*
- c) WBP Group provides a simple means by which the individual may easily request not to receive direct marketing communications from WBP Group; and
- d) in each direct marketing communication with the individual:

WBP Group Privacy Policy

- i. the WBP Group includes a prominent statement that the individual may make such a request; or*
 - ii. WBP Group otherwise draws the individual's attention to the fact that the individual may make such a request; and*
- e) the individual has not made such a request to WBP Group.

Social Media

WBP Group may use personal information other than sensitive information associated with social media marketing or activities in line with the direct marketing provisions above.

STORAGE OF PERSONAL INFORMATION

WBP Group endeavor to protect the security of your personal information. Your personal information is stored in a manner that reasonably protects it from misuse, interference, loss and from unauthorised access, modification or disclosure.

When your personal information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your personal information. However, most of the personal information we collect or store is, or will be, retained for as long as required by applicable law.

CONSENT

By providing any personal information to us, you provide unequivocal consent for the information to be collected, used or disclosed in accordance with this policy.

ANONYMITY

If you do not wish for your personal information to be disclosed or used in such a way anticipated by this Privacy Policy, we will use reasonable endeavors to accommodate your request where the disclosure is not otherwise required by law or mandated industry requirements. If we comply with your request, it may not be practicable for us to provide you some or all of the services that would otherwise be available. If you wish to make a request, you can email: privacy@wbpgroup.com.au or put this in writing addressed to the National Compliance and Risk Manager.

WBP Group Privacy Policy

LINKS TO THIRD-PARTY WEBSITES

WBP Group make no representation as to the security, collection, use or disclosure of any personal information as a result of other third-party websites which may be linked to that of WBP Group. Where third party websites are used, this is done entirely at the risk of the user.

COMPLAINTS

Making a complaint

You may make a complaint if you consider that the WBP Group has interfered with your privacy because of an alleged breach of the privacy principles under the Privacy Act. A complaint may be made by completing the provided form and emailing this to: complaints@wbpgroup.com.au

Our National Compliance and Risk Manager will investigate the issue and determine the steps that we will undertake to resolve your complaint. We will contact you if we require any additional information from you and will notify you in writing of the outcome of the investigation.

WBP Group will keep a record of all complaints and determinations together with a record of the action taken to remedy any breach.

If you are not happy with the outcome you can:

- a) Take the complaint to an external dispute resolution scheme where applicable
- b) Make the complaint to the Office of the Australian Information Commissioner
<https://www.oaic.gov.au/individuals/how-do-i-make-a-privacy-complaint>

ACCESS TO, AND CORRECTION OF PERSONAL INFORMATION

If you want to access, or correct personal information held by WBP Group, you can email make the request to do so by emailing: privacy@wbpgroup.com.au

In accordance with the Privacy Act, there may be circumstances where WBP Group may not be able to provide access to this information.

RESOURCES

The Privacy Act 1988^{Cth}

Privacy Amendment (Notifiable Data Breaches) Act 2017^{Cth}

The Office of the Australian Information Commissioner (various publications and resources)

WBP Group Privacy Policy

PRIVACY AMENDMENT ACT 2017- NOTIFIABLE DATA BREACHES (NDB SCHEME)

NDB OVERVIEW

WBP Group are committed to compliance with The Privacy Amendment Act 2017 (Notifiable Data Breaches or NDB Scheme) including notification requirements, investigating if there is an eligible data breach and, if so, if 'serious harm' is considered likely.

The NDB scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'.

SERIOUS HARM

Upon notification of an apparent 'data breach', WBP Group are committed to investigate and establish, from the perspective of a 'reasonable person', if the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach and as such constitutes an eligible data breach. WBP Group are committed to assess the likelihood of 'serious harm' and have a Data Breach Response Plan in place incorporating a Data Breach Response Team.

PREVENTING SERIOUS HARM WITH REMEDIAL ACTION

In accordance with the NDB scheme, WBP Group may avoid the need to notify if positive steps to address a data breach in a timely manner are taken.

- a) If WBP Group takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity (s 26WF(1), s 26WF(2), s 26WF(3)).
- b) For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information (s 26WF(3)). If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

WBP Group Privacy Policy

MINIMISATION OF SERIOUS HARM BY RESTRICTION OF INFORMATION HELD

WBP Group are committed to not retaining sensitive or potentially sensitive information unnecessarily.

Specifically, unless circumstantially located within documents required to be retained by law or industry best practise for file purposes, it is WBP Group Policy not to unnecessarily retain sensitive information.

NOTIFICATION

WBP Group are committed to compliance with legislative notification requirements under the Privacy Amendment Act 2017 and have a Data Breach Response Plan which will be implemented in the event of an eligible data breach. WBP Group's commitment to compliance with notification requirements forms part of the Data Breach Response Plan.