

# Privacy Policy

8 November 2017

## 1 Introduction

### 1.1 RMCG WILL RESPECT YOUR PRIVACY

RMCG is committed to providing quality services to its clients and this policy outlines our ongoing obligations in respect of how we manage personal information. We will treat all personal information we hold with respect and appropriate care and security and we commit to not releasing information obtained to external parties, unless prior written consent is received. If at any time, RMCG is required by law, to release information about an individual or organisation, we will meet this obligation.

We will ensure that all employees are familiar with this policy and understand the actions required for its implementation. We will do this by providing the necessary training and education via induction (for new employees) and discussion at internal staff meetings (for existing employees).

We have adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The APPs govern the way we collect, use, disclose, store, secure and dispose of personal information.

Strictly, the Privacy Act only applies to personal information relating to individuals and so does not apply to information about businesses, organisations or partnerships. This policy confirms that RMCG will apply the same strict controls to any information that we collect or hold about individuals or clients, to businesses, organisations or partnerships, whatever their size or standing.

A copy of the Australian Privacy Principles can be found in Appendix 1.

## 2 External information and data

### 2.1 WHAT SORT OF INFORMATION DOES RMCG COLLECT AND WHY?

During our work, we collect information to enable us to advise clients, according to their instructions or brief, on how to effectively achieve required outcomes. That data may include sensitive or confidential information about an individual or organisation.

Examples of personal information we collect include but may not be limited to: names, addresses, email addresses, phone and facsimile numbers. Examples of information about organisations we collect include but may not be limited to: size of organisation, number of employees, area (e.g. of farms), spatial data (GIS/GPS), production data, financial data, data about resource use. Information about organisations is, in many cases, covered by individual confidentiality agreements.

This information is obtained in many ways including: email, telephone, face-to-face meetings, interviews, correspondence, through our website or from third parties.

### 2.2 HOW DOES RMCG USE DATA?

From time to time, projects being undertaken by RMCG, require personal information to be obtained to support analysis and recommendations provided to clients. Reports and advice to clients will generally be confidential to that client, therefore sensitive or personal information will only be disclosed back to the client that provided the data.

Where industry-wide studies are undertaken involving benchmarking or similar research, then data will only be released or published that is either:

- With the permission of the individual or enterprise concerned
- Anonymous, with care to protect against inadvertent identification of an individual
- On an aggregate basis, i.e. across sufficient entities to limit the chance for data to be identified with a specific individual or enterprise

### 2.3 HOW WILL RMCG KEEP YOUR PERSONAL / ORGANISATIONAL INFORMATION SECURE?

When we collect personal information or information about an organisation, we will, where appropriate and where possible, explain why we are collecting the information and how we plan to use it.

RMCG holds personal information in hardcopy and/or electronic formats and in a manner that reasonably protects it from misuse and loss and from unauthorized access,

modification or disclosure. These include secured and controlled business premises and IT networks that prevent external access and limit internal access to persons directly involved in the delivery of a contracted service. The security of data and information is part of our formal Quality Management System.

When personal/organisational information is no longer required for the purpose for which it was obtained, we will take reasonable steps to destroy it (via security shredding), file it securely (both electronically and hardcopy) as per section 2.3 and, if requested, return the information to the individual/organisation who originally supplied it (hardcopy only).

## **2.4 WHAT CONTROLS DOES RMCG USE TO ENSURE PRIVACY?**

RMCG has the following arrangements in place to meet best practice in privacy controls:

- We will only collect personal/organisational information that is needed for our work
- When we collect personal information from individuals we will notify them of our privacy policy when requested (or it is accessible via our website).
- We will only use personal information for the primary purpose for which it was originally collected, unless we have permission from the individual for any other use
- We will maintain effective security arrangements to protect personal information (2.2)
- We will only disclose that information with the permission of the individual/organisational to whom it refers.

## **2.5 ACCESSING, CORRECTING & UPDATING YOUR PROFILE**

We will take reasonable steps to make sure that personal information is accurate, complete and up-to-date. If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide quality services to you.

# **3 Internal information and data**

## **3.1 PROTECTING INTERNAL PERSONAL INFORMATION**

Within RMCG we operate within a culture of openness, trust and mutual respect. That applies both to personal contact across the office and access to personal information via our ICT systems.

RMCG follows the same controls to protect internal personal information as it does for external information, however also expects the following approach by all employees in maintaining the privacy of information about others within the business.

- Think about the information that you hold and know about other people in the business

- Respect that knowledge and information
- Keep personal information confidential
- Implement sensible controls to keep information confidential
- Don't look at things that you don't need to look at

This approach helps maintain the open culture of trust and mutual respect we value.

## 4 Complaints

Please let us know if you believe that confidential personal information that we hold has been collected, used or disclosed in a way that breaches this Privacy Policy. We want to ensure that we meet best practice in the way we operate.

Any complaint or enquiry will be dealt with initially by our Privacy Officer. The issues raised will be assessed and responded to, normally within five working days.

If you believe the response is unsatisfactory, then your concern and our response will be reviewed by one of the Directors of RMCG, selected as independent from the work related to the complaint. We will respond to you with the outcome of that review within five working days of receiving your further complaint.

If you are unhappy about our response and further review then you have the right at any time to refer the matter to the Australian Information Commissioner at the contact details below:

Australian Information Commissioner

Phone: 1300 363 992  
Fax: (02) 9284 9666  
Email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)  
Post: GPO Box 5218, Sydney, NSW 2001

### Contacting RMCG

If you have any questions about this Privacy Policy, you should contact:

Business Manager

RMCG Privacy Officer

Phone: (03) 5441 4821  
Email: [rm@rmcg.com.au](mailto:rm@rmcg.com.au)  
Post: 135 Mollison Street, Bendigo Victoria 3550

# Appendix 1: Australian Privacy Principals



## Australian Privacy Principles — a summary for APP entities

from 12 March 2014



**APP 1 — Open and transparent management of personal information**  
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

**APP 2 — Anonymity and pseudonymity**  
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

**APP 3 — Collection of solicited personal information**  
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

**APP 4 — Dealing with unsolicited personal information**  
Outlines how APP entities must deal with unsolicited personal information.

**APP 5 — Notification of the collection of personal information**  
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

**APP 6 — Use or disclosure of personal information**  
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

**APP 7 — Direct marketing**  
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

**APP 8 — Cross-border disclosure of personal information**  
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

**APP 9 — Adoption, use or disclosure of government related identifiers**  
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

**APP 10 — Quality of personal information**  
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

**APP 11 — Security of personal information**  
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

**APP 12 — Access to personal information**  
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

**APP 13 — Correction of personal information**  
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

**For private sector organisations,  
Australian Government  
and Norfolk Island agencies  
covered by the Privacy Act 1988**

[www.oaic.gov.au](http://www.oaic.gov.au)