

	Policy Manual P2 People HRMS	Issue Date:	March 2019
		Issue Status:	Issue 6
		Authorised By:	Peter O'Brien, CEO
Section F – Employment Standards			

F.5. Privacy Policy

Related Policies	<ul style="list-style-type: none"> ▪ Code of Conduct ▪ Electronic Systems Usage and Communication ▪ Social Media
Related Documents	<ul style="list-style-type: none"> ▪ Australian Privacy Principles
Attachments	<ul style="list-style-type: none"> ▪ Nil

1. Introduction

OMC International respects the privacy rights of all individuals in the workplace and is committed to ensuring that the Chief Executive Officer (CEO), all managers and employees working at OMC International comply at all times with their obligations under the *Privacy Act 1988 (Cth)* and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*, including the *Australian Privacy Principles 2014*.

Policy purpose: This *Privacy Policy* summarises the standards of privacy and confidentiality applicable at OMC International. It is to be used as a guide by Managers and employees to set up and maintain systems and procedures that promote ethical and professional conduct.

Policy scope: This Policy applies to all persons including: senior officers; full-time, part-time, casual employees and contractors who are engaged to work at any OMC International locations and at any other locations on behalf of OMC International. They are collectively referred to as employees in this Policy, unless specifically referenced.

Employees based outside of Australia will be required to apply the procedures outlined in this Policy when working and communicating with Australian based employees and must also comply with any applicable home country law when applying these procedures in their home country.

2. Australian Privacy Principles

The Australian Privacy Principles (APP) established by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* applies to all organisations and Government agencies. OMC International therefore adheres to the principles as set out in the APP in the way it collects, manages and uses information provided to the company from employees, other parties associated with OMC International.

3. International Privacy Principles

OMC and its suppliers aim to comply with all applicable privacy laws to which it is subject.

4. Collection of Information

OMC International collects personal information from a number of sources for varying reasons. Personal information is only collected by lawful means where it is necessary for OMC International to collect and use this information.

Personal information is only collected directly from the individual concerned.

At the time of collection, the individual will also be informed as to the purpose for the collection of the information and that they are able to access any information provided to OMC International.

5. Data Security

OMC International undertakes to adequately protect the personal information held by the company from misuse, loss and unauthorised access, modification or disclosure.

All employees are required to respect private information held by the company and to ensure all company procedures in relation to the security of information are adhered to.

Unauthorised access, misuse, modification or disclosure of this personal information held by the company by any of its employees will be considered a serious breach of company policy and will lead to appropriate disciplinary action.

Employees will be regularly reminded and advised of changes in the company procedures for management and security of personal information. If an employee is unsure of any of these procedures or are unsure in a particular situation then they must initially consult their line manager for guidance.

6. Use and Disclosure

OMC International will only use personal information it collects for its original purpose which is disclosed at the time of collection. However, the company may disclose personal information it holds where there is a legal duty to do so, including circumstances where a lawful duty of care to disclose information exists.

Personal information collected may be disclosed to other branches/sections and trusted suppliers within the company provided it is used in a manner which is in line with its original purpose of collection and use.

Where the information provided it is used to communicate with a client, the client will be provided with the opportunity to decline receiving communication from the company.

6.1 Type of Personal Information Held

Personal and/or sensitive information that is collected and held by OMC International usually falls into the following categories:

Clients

- Client contact and client details
- Information regarding products and services the client offers
- Information regarding how the client interacts with OMC International
- Previous dealings with the client, which may include meeting notes and information obtained through the provision of products and services
- Contact names of individual employees of the client obtained through dealings.

Potential/Existing Employees

- Candidate information submitted and obtained from the candidate and other sources in connection with applications for employment
- Employment performance information
- Employee information e.g. home address and contact details, sex, date of birth
- Information about incidents in the workplace
- Information obtained to assist in managing client and business relationships
- Information documenting the work history of these workplace participants (such as their letter of appointment and bank account details as well as records of any salary adjustments).

6.2 Purposes for Which Personal Information is Held

There is a variety of reasons why OMC International is required to hold personal information. Primarily these reasons include:

- For contact purposes
- To comply with legislation and government requirements
- To set up clients' accounts
- To identify clients when they request services or change their details
- To answer client queries
- To ensure the continual improvement of OMC International, its employees and its products and services offered
- To customise advertising and marketing content
- To conduct research and collect statistics.

When clients subscribe to OMC International's services, they consent to their personal details being used to establish their account.

7. Access

Subject to some exceptions that are set out in the National Privacy Principles, all persons may gain access to their personal information that is held by OMC International. Access may be refused, if it would interfere with the privacy rights of other persons or if it breached any confidentiality that attaches to that information.

Access to another person's personal information will not be provided in any circumstances except:

- An agent that a client/employee has provided consent to requests such information
- Where we are required to by law
- If we believe it is necessary to protect OMC International property or rights, another OMC International customer or a member of the public
- To another party if we sell our company or part its business to that other party.

8. Data quality

On a regular basis OMC International will make a request directly to individuals for them to check and update records of their personal information.

9. Information Destruction Policy

OMC International holds all required personnel information for a period of 7 years.

All non-current information or information deemed no longer to be required by OMC International shall be destroyed. Items shall be destroyed by being placed into a security destruction bin and removed from the premises of OMC International.

Prior to destruction, notations from the information may be made for later reference.

10. Complaints

Anyone who feels that there has been an unwarranted invasion of their privacy should contact the CEO at OMC International.

11. Notifiable Data Breach Scheme

Whilst OMC International will endeavour maintain compliance with the Privacy Act at all times, if there is an incident/breach then the following procedure should be followed which is in line with the Notifiable Data Breaches Scheme.

- Maintain information governance and security according to the F.5 Privacy Policy clause 4
- Contain a suspected or known breach where possible
- Assess using 3 stages:
 1. Initiate: plan the assessment and assign a team or person
 2. Investigate: gather relevant information about the incident to determine what has occurred

3. Evaluate: make an evidence-based decision about whether serious harm is likely. Document your findings and decision within 30 days

If serious harm is still likely, complete statement for the Commissioner available on the Commissioner's website <https://www.oaic.gov.au/>

If no serious harm is likely, review the incident and take action to prevent future breaches.

Refer; Appendix A – K&L Gates Notifiable Data Breaches Scheme document for more details on this process.

Where to go for more information

Australian Privacy Principles 2014 - www.oaic.gov.au

Legislation

Privacy Act 1988 (Cth) - www.comlaw.com.au

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) – www.comlaw.gov.au

Victoria

Information Privacy Act 2000 (VIC) – www.legislation.vic.gov.au

Western Australia

Privacy Act 1988 (WA) – www.slp.wa.gov.au

OMC International ONLY:	
Document:	Privacy Policy
Last Date Issued:	May 2016
Next Review Date:	May 2017
Issue Number:	4
Developed by:	Shave Human Resources
Authorised by:	Peter O'Brien, Chief Executive Officer

RECORD OF REVISIONS:				
Revision	Date	Section	Page	Details
Issue 1	October 2013	All	All	Original
Issue 2	May 2014	1 & legislation	1 & 3	Updated with legislative changes as per Executive Summary May 2014
Issue 3	May 2015	Administrative only		Refer Executive Summary 1 May 2015
Issue 4	May 2016	Administrative only		Refer Executive Summary 1 May 2016
Issue 5	June 2018	All	All	Refer to table of contents, Workfront number 106209
Issue 6	March 2019	3 & 6	1 & 2	Refer to workfront request 136056

Appendix A.



NOTIFIABLE DATA BREACHES SCHEME

When does the scheme begin?

From 22 February 2018 many business and Commonwealth government agencies will be required to comply with the new notifiable data breaches scheme (NDB Scheme).

Do I need to comply with the scheme?

If you are currently bound to comply with the Australian Privacy Principles, you will be required to comply with the NDB Scheme.

Briefly, what is the scheme all about?

Prior to the introduction of the NDB Scheme in Australia, notification of a data breach to the Australian Information Commissioner was not mandatory under the *Privacy Act 1988* (Cth).

Under the NDB Scheme, an APP Entity will be required to notify the Commissioner and affected individuals of a data breach that is likely to result in serious harm to those affected individuals.

Why is it important to prepare for the scheme?

Failure to comply with the NDB Scheme may attract a civil penalty (currently up to AUD420,000 for individuals and AUD2.1 million for corporations). The Commissioner has also evidenced a willingness to pursue enforceable undertakings.

The regular occurrence of data breaches over the past few years is a constant reminder that data

What do I need to do to prepare?

At a minimum, you should make an upfront investment to prepare for the scheme by:

- reviewing your current privacy and data security policies and procedures and incident/breach response plans.
- assessing whether your policy and procedures set out a plan you can follow in the event you suffer a data breach. We recommend all clients work up a clear breach response plan. The Commissioner expects it and our clients have all found it so much more effective to have pre-thought out a crisis response. If you do not have a data breach response plan, we recommend you prepare one to allow you to comply with the NDB Scheme.
- increasing staff awareness of your information security policies and procedures and conducting staff training to inform all staff members of the new NDB Scheme. Remember, it is everyone's responsibility to remain vigilant and know what to do if they become aware of a data breach.

breaches are costly to businesses and can have significant wide reaching operational, financial, legal and reputational consequences.

Contact



Cameron Abbott

Partner

+61 3 9640 4261

Cameron.Abbott@klgates.com



Warwick Andersen

Special Counsel

+61 2 9513 2508

Warwick.Andersen@klgates.com



Rob Pulham

Senior Associate

+61 3 9640 4414

Rob.Pulham@klgates.com



Keely O'Dowd

Senior Associate

+61 3 9640 4308

Keely.O'Dowd@klgates.com