OMC INTERNATIONAL	**Policy Manual** **P2** **People** **HRMS**	**Issue Date:**	**June 2018**
		Issue Status:	**Issue 5**
		Authorised By:	**Peter O'Brien, CEO**
Section F – Employment Standards			

F.5. Privacy Policy

Related Policies	▪ Code of Conduct ▪ Electronic Systems Usage and Communication ▪ Social Media
Related Documents	▪ Australian Privacy Principles
Attachments	▪ 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 aims 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 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, it's 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

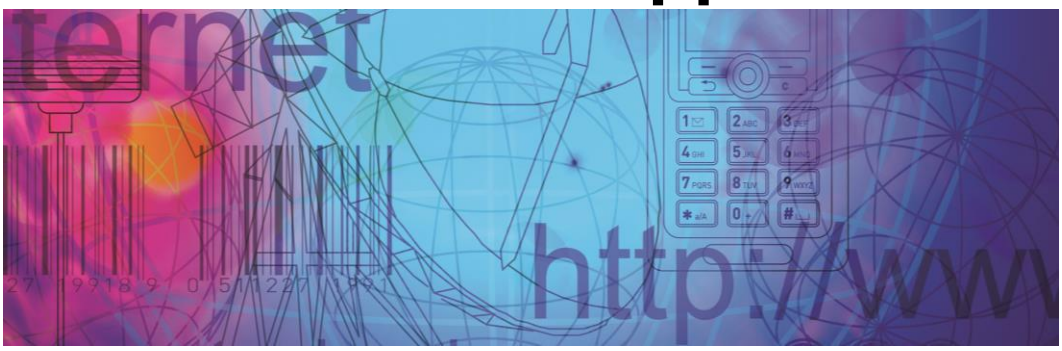
Privacy Act 1988 (WA) – www.slp.wa.gov.au

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

Appendix A.

K&L GATES



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

K&L GATES

Data Breach Response Summary

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate**: plan the assessment and assign a team or person
- **Investigate**: gather relevant information about the incident to determine what has occurred
- **Evaluate**: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

Is serious harm still likely?

NO

YES

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- Police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider.

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Source: Office of the Australian Information Commissioner