Australasian Security Risk Management

PRIVACY POLICY

ASRM Pty Ltd (ASRM) is bound by the ***Information Privacy Act 2000*** in how it manages personal information. ASRM is committed to protecting the personal information of clients with whom it interacts with during its functions and activities.

1 WHAT IS PERSONAL INFORMATION?

1.1 Personal information means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion, but does include health information. Health information is governed by the ***Health Records Act 2001.***

1.2 The type of information collected by ASRM includes names, date of birth, address, contact details, sex and records. This information is collected because of the legitimate business activities associated with ASRM and is recorded in paper or electronic form.

1.3 ASRM supports the regulation of personal information privacy, however, there will be situations where to meet the needs of a client, ASRM collect, use and/or disclose personal information. Such use will, in most cases, be with the consent of the client.

1.4 This document outlines the Service's policies regarding the management of personal information.

1.5 ASRM is required to comply with the Information Privacy Principles (IPP's) unless it is reasonably necessary not to. **Section 13, *Information Privacy Act 2000*** creates exemptions for ASRM whereby it is not necessary to comply with some IPP's if it is believed on reasonable grounds that non-compliance is necessary pursuant to its policies, for example,

- reporting the commission of a crime such as fraud or deception.
- Activities in connection with the conduct of proceedings commenced, or about to be commenced in any court or tribunal.

1.6 It should be noted that the IPP's may not apply if there is specific provision in another Act that applies to the handling of information which conflicts with the IPP's. If there is a conflict, then the specific provision takes precedence.

The Information Privacy Act 2000 consists of ten (10) IPP's. The following is a summary of how ASRM manages your privacy information.

Principle 1 – Collection

It is necessary for ASRM to collect personal information in order to carry out its functions and activities. ASRM will only collect personal information by lawful and fair means.

Where ASRM collects personal information for purposes not associated with its security functions, persons from whom the information is collected, will be advised how their information will be used and/or disclosed and how they can gain access to their information.

Principle 2 – Use and Disclosure

The ***Information Privacy Act 2000*** provides that personal information should only be used or disclosed for the primary purpose for which it was collected. It should only be used or disclosed for a secondary purpose that would be reasonably expected or if consent has been obtained. On some occasions where ASRM believes on reasonable grounds that it is necessary; it can use or disclose personal information for reasons other than that for which it was collected. The ***Information Privacy Act 2000*** provides exemptions in situations where this is necessary.

In general, ASRM only uses or discloses personal information in order to carry out its core functions. However, ASRM may where it is reasonably believed to be necessary, use or disclose the personal information it collects for a purpose that is different from the original reason the personal information was collected. This would include the following situations: -

- ASRM reasonably believes that the use or disclosure is necessary to lessen or prevent
  - A serious and imminent threat to an individual's life, health, safety or welfare

- ASRM has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information in reporting its concerns to relevant persons or authorities, or

- The use or disclosure is required or authorized by or under law.

- ASRM reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency –
  - The protection of public revenue.
  - The prevention, detection, investigation or remedying of any improper conduct.
  - The preparation for or conduct of, proceedings before any court or tribunal, or implementation of orders of a court or tribunal.

Principle 3 – Data Quality

ASRM takes reasonable steps to ensure that the personal information it collects uses or discloses is accurate, complete and up to date.

Principle 4 – Data Security

Personal information held by ASRM must be protected from misuse, loss, unauthorized access, modification and disclosure. All personal information held by ASRM is kept in a secure environment and made available only to authorized personnel who have a demonstrated need to access the information.

Principle 5 – Openness

ASRM has clearly expressed, publicly available policies on the way it manages personal information. The statement provides an overview of the Service's policies regarding the management of personal information.

Principle 6 – Access and Correction

Individuals can request access to personal information about themselves held by the Service. If individuals believe their personal information is inaccurate, incomplete or out of date the

individual is entitled to request that it be corrected. There may be circumstances where access to information cannot be granted as it may compromise the privacy of another individual. Section 33 of the *Freedom of Information Act 1982* exempts from release any information which relates to the personal affairs of any person. All access should be sought through the *Freedom of Information Act 1982*. Such requests may be made in writing to the General Manager.

Principle 7 - Unique Identifiers

Unique identifiers, usually a number, are utilized by ASRM to enable ASRM to carry out its functions efficiently.

Principle 8 – Anonymity

If it is lawful and practicable, a person must have the option of not identifying themselves when entering transactions with the Service.

Principle 9 – Trans-border Data Flows

Pursuant to the *Information Privacy Act 2000* an organization that is transferring personal information to another organization outside Victoria must ensure that the receiving organization has equivalent privacy protection, and that the information transferred will be protected.

Principle 10 – Sensitive Information

This includes racial or ethnic origin, political views, religious beliefs and sexual preferences, memberships of groups or criminal records. There are special restrictions on the collection of this information.

2 Complaints

2.1 If a person wishes to lodge a complaint a breach of privacy, such complaint should be directed to: -

Privacy Victoria
Level 11, 10-16 Queen Street,
Melbourne Victoria 3000
GPO box 5057
Melbourne Victoria 3001
Telephone: 1300 666 444