



## PRIVATE SECTOR INFORMATION SHEET 7 – 2001 *Unlawful Activity and Law Enforcement*

The *Privacy Act 1988* (Cth) (the Privacy Act) seeks to balance the privacy of individuals with the public interest in law enforcement and the regulatory objectives of government. In the course of carrying out their activities and functions, enforcement bodies, government agencies and regulatory authorities collect personal information from organisations. This paper sets out the circumstances in which, for law enforcement or regulatory purposes, an organisation can use or disclose personal information under National Privacy Principle 2 (NPP 2) and deny access to personal information under NPP 6.

### Use and disclosure for law enforcement and regulatory purposes

NPP 2 establishes the general rule that personal information must only be used or disclosed for the primary purpose for which it was collected. However, there are exceptions to the general prohibition against use and disclosure for secondary purposes, which permit an organisation to use and disclose personal information for law enforcement and regulatory purposes. These exceptions are set out in NPP 2.1 (f), (g) and (h).<sup>1</sup>

The Privacy Act is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions.<sup>2</sup> Police and other enforcement bodies are generally reliant on the voluntary cooperation of organisations to provide information.

It should also be noted that the Privacy Act is not intended to interfere with legal obligations that organisations might already have which affect the use and disclosure of personal

information. For example, NPP 2.1 does not override the duty of confidentiality between a medical practitioner and patient. Furthermore, an organisation is entitled not to disclose personal information if there is no law that requires it.<sup>3</sup>

### Use or disclosure for reporting or investigating unlawful activity – NPP 2.1 (f)

NPP 2.1(f) allows an organisation to use or disclose personal information when it has reason to suspect that unlawful activity has been, is being or may be engaged in. 'Unlawful activity' refers to acts or omissions that are expressly prohibited by Commonwealth, State or Territory law. NPP 2.1(f) requires a factual basis for suspecting unlawful activity. The suspected unlawful activity will ordinarily relate to the operations of the organisation.

A further requirement for relying on NPP 2.1(f) is that:

- the use or disclosure of personal information is a necessary part of an organisation's investigation of the unlawful activity; or
- the use or disclosure occurs in the context of the organisation reporting its concerns to relevant persons or authorities.

If an organisation cannot effectively investigate or report suspected unlawful activity without using or disclosing personal information, then the use or disclosure would be regarded as necessary to investigating or reporting the unlawful activity.

'Relevant persons or authorities' to which an organisation may report unlawful activity include but are not limited to:

<sup>1</sup> NPP 2, Schedule 3, *Privacy Act 1988*

<sup>2</sup> Note 1 to NPP 2, Schedule 3, *Privacy Act 1988*

<sup>3</sup> Note 2 to NPP 2, Schedule 3, *Privacy Act 1988*

- 'enforcement bodies' as defined in section 6(1) of the Privacy Act;
- agencies and regulatory authorities such as Austrac and State and Territory Departments of Fair Trading and Offices of State Revenue;
- self-regulatory authorities such as the Australian Stock Exchange, the Telecommunications Industry Ombudsman and the Banking Industry Ombudsman.

### Use or disclosure required or authorised by law – NPP 2.1 (g)

The Privacy Act does not override legal obligations to use or disclose personal information. NPP 2.1(g) provides that an organisation can use or disclose personal information where this is required or authorised by law. 'Law' includes Commonwealth, State and Territory legislation, as well as the common law.

'Required by law' covers circumstances in which there is a legal obligation to use or disclose personal information in a particular way. Examples include:

- a warrant, order or notice issued by a court for the provision of information, or the production of books, records or documents held by an organisation for inspection;
- a warrant, order or notice issued by a government agency and/or enforcement body for the provision of information, or the production of books, records or documents held by an organisation for inspection;
- statutory requirements to report matters to agencies or enforcement bodies such as:
  - the reporting of specific financial transactions to Austrac under the *Financial Transactions Reports Act 1988* (Cth);
  - the reporting of notifiable diseases by health service providers to health authorities;
  - suspected cases of child abuse to relevant authorities; and
- legislation that requires an organisation to carry out some action, which of necessity involves particular uses or disclosures of personal information.

'Authorised by law' refers to circumstances where the law permits but does not make it compulsory for an organisation to make a use or disclosure. The word 'authorised' indicates that

an organisation has some discretion as to whether or not to make a use or disclosure.

### Use and disclosure in relation to enforcement bodies – NPP 2.1 (h)

NPP 2.1 allows an organisation to use or disclose personal information where the organization reasonably believes that the use or disclosure is reasonably necessary for a range of functions or activities carried out by, or on behalf of, an enforcement body. A 'reasonable belief' is a belief that might reasonably arise in the circumstances based on the facts of the situation. A use or disclosure might be considered 'reasonably necessary' if an enforcement body cannot effectively carry out its functions (as specified in NPP 2.1(h)(i) to (v)) without the organisation using or disclosing personal information.

Section 6(1) of the Privacy Act defines enforcement bodies as:

- the Australian Federal Police;
- the National Crime Authority;
- the Australian Customs Service;
- the Australian Prudential Regulation Authority (APRA);
- the Australian Securities and Investments Commission (ASIC);
- Commonwealth, State and Territory agencies responsible for administering or performing a function under a law that imposes a penalty or sanction;
- Commonwealth, State and Territory agencies responsible for administering a law relating to the protection of public revenue;
- State or Territory police services;
- the New South Wales Crime Commission;
- the Independent Commission Against Corruption of New South Wales;
- the Police Integrity Commission of New South Wales;
- the Criminal Justice Commission of Queensland; and
- State and Territory authorities responsible for conducting criminal investigations or inquiries and prescribed under the Privacy Act. (At this stage, no authorities have been prescribed.)

### The enforcement of criminal law

NPP 2.1(h)(i) provides that an organisation can use or disclose personal information where it

reasonably believes that it is reasonably necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences by an enforcement body. A criminal offence is an act or practice that is prohibited by criminal law at Commonwealth or State and Territory level.

## Law imposing a penalty or a sanction

NPP 2.1(h)(i) enables an organisation to use or disclose personal information for the enforcement of a law imposing a penalty or a sanction. 'Penalty' generally means a punishment imposed for a breach of law that is of a pecuniary nature, such as a fine or monetary payment. 'Sanction' generally refers to a punishment for a breach of law involving the refusal or withdrawal of a benefit. A 'law imposing a penalty or sanction' is not confined to instances where a breach of the law may result in a criminal conviction. It includes a law that allows the Government to refuse a benefit or impose other non-criminal consequences for failure to comply with a legal obligation, such as a refusal to grant a visa or licence, revocation of a visa or licence, imposition of civil penalties or other administrative orders prohibiting or requiring certain things.<sup>4</sup>

## Laws relating to the confiscation of the proceeds of crime

NPP 2.1(h)(ii) enables organisations to use or disclose information where it is reasonably necessary for the enforcement of laws relating to the confiscation of the proceeds of crime. Examples of legislation of this kind include the *Proceeds of Crimes Act 1987* (Cth), the *Confiscation of Proceeds of Crime Act 1989* (NSW), the *Criminal Assets Recovery Act 1990* (NSW) and the *Proceeds of Crimes Act 1991* (ACT). These laws enable enforcement bodies to trace the proceeds, benefits and property derived from criminal activity, and provide for the forfeiture of property used in connection with the commission of criminal offences. They provide for the enforcement of forfeiture orders, pecuniary penalty orders and restraining orders made in respect of offences against the laws of other jurisdictions.

## The protection of public revenue

NPP 2.1(h)(iii) permits an organisation to use or disclose personal information where this is reasonably necessary for the protection of public revenue by an enforcement body. Public revenue refers to taxes, levies and charges collected by Commonwealth, State, Territory and Local Governments. Protecting public revenue includes those activities directed to ensuring that organisations or persons comply with their legal obligations under taxation and other forms of public revenue law.

## Seriously improper conduct

NPP 2.1(h)(iv) provides that an organisation may use or disclose personal information where this is reasonably necessary for the prevention, detection, investigation or remedying of seriously improper conduct. 'Seriously improper conduct' refers to serious breaches of standards of conduct associated with a person's duties, powers, authority and responsibilities. It includes corruption, abuse of power, dereliction of duty, breach of obligations that would warrant the taking of enforcement action by an enforcement body or any other seriously reprehensible behaviour.

## Proceedings in a court or tribunal

NPP 2.1(h)(v) allows an organisation to use or disclose personal information for the preparation or conduct of proceedings before any court or tribunal by an enforcement body.<sup>5</sup> It also enables an organisation to use or disclose information to implement orders issued by the court or tribunal.

## Written note of use or disclosure – NPP 2.2

NPP 2.2 requires an organisation that uses or discloses personal information under NPP 2.1(h) to make a note of that use or disclosure. Details that the organisation could usefully note include:

- the date of the use or disclosure;
- the personal information used or disclosed;
- the relevant enforcement body; and
- how the information was used or to whom the information was disclosed.

---

<sup>4</sup> For example, imposing conditions on licences.

---

<sup>5</sup> For example, a class action conducted by ASIC to recover damages or property where it is in the public interest.

The requirement to make a note does not apply where a law prohibits the organisation from making such a record.

### Tips for compliance

There are several measures that an organisation could adopt to ensure that it complies with NPPs 2.1(f), (g) and (h). These include:

- developing procedures for using and disclosing personal information for the purposes of investigating and reporting suspected unlawful activity, meeting legal requirements and assisting enforcement bodies;
- making a senior person within an organisation responsible for deciding to release information. For example, the disclosure of personal information in accordance with NPP 2.1(g) could be subject to an assessment of the scope of a warrant, order or notice by a senior person in order to ensure that the organisation does not release more personal information than is necessary.

### Denying access to personal information

If a person asks an organisation for access to personal information about them, an organisation must give access under NPP 6. However, NPP 6 does not override legal obligations that prevent access. Nor is NPP 6 intended to interfere with the investigation of unlawful activity or the activities of enforcement bodies.

### Providing access where unlawful – NPP 6.1(g)

NPP 6.1(g) allows an organisation to deny a person access to personal information about them if giving access would be unlawful. For example, this would cover circumstances where giving access would be a breach of confidence.

### Denying access required or authorised by law – NPP 6.1(h)

NPP 6.1(h) provides that an organisation can deny access when required or authorised by

Commonwealth, State or Territory legislation or the common law. 'Required by law' means that an organisation must deny access. 'Authorised by law' refers to a law that gives an organisation the discretion to deny access.

### Access likely to prejudice investigation of possible unlawful activity – NPP 6.1(i)

Organisations have a legitimate function in investigating and reporting unlawful activity. NPP 6.1(i) allows an organisation to deny access when unlawful activity is being investigated and providing access would prejudice the investigation.

### Access likely to prejudice activities of enforcement bodies – NPP 6.1(j)

NPP 6.1(j) permits an organisation to deny access to an individual when this would prejudice activities being carried out by, or on behalf of, an enforcement body. These activities are:

- the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
- the enforcement of laws relating to the confiscation of the proceeds of crime;
- the protection of public revenue; or
- the preparation for, or conduct of proceedings before any court or tribunal, or implementation of its orders.

### Access likely to cause damage to security of Australia – NPP 6.1(k)

NPP 6.1(k) allows an organisation to deny access to an individual when an enforcement body performing a lawful security function asks the organisation not to provide access to personal information on the basis that providing access would be likely to cause damage to the security of Australia.

## Private Sector Information Sheets

Information sheets are advisory only and are not legally binding. The National Privacy Principles in Schedule 3 of the Privacy Act do legally bind organisations.

Information sheets are based on the Office of the Privacy Commissioner's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation. Nothing in an information sheet limits the Privacy Commissioner's ability to investigate complaints under the Privacy Act or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with. Organisations may also wish to consult the Commissioner's guidelines and other information sheets.

## Office of the Privacy Commissioner

Privacy Enquiries Line **1300 363 992** - local call (calls from mobile and pay phones may incur higher charges)  
TTY 1800 620 241 – no voice calls; Fax + 61 2 9284 9666; GPO Box 5218, Sydney NSW 2001.

Private Sector Information Sheet 7  
Web HTML, Word and PDF published December 2001  
ISBN 978-1-877079-29-4  
© Commonwealth of Australia

**[www.privacy.gov.au](http://www.privacy.gov.au)**