Australian Government

Office of the Privacy Commissioner

# PRIVATE SECTOR INFORMATION SHEET 30 – *ID scanning in pubs and clubs*

This Information Sheet is for private sector hospitality organisations like clubs and pubs that are covered by the Privacy Act (s 6C) and are:

- collecting personal information using scanning devices, or
- considering using scanning devices.

Clubs and pubs must comply with the National Privacy Principles (NPPs) when handling personal information.

Personal information includes 'identity information' such as a driver's licence, proof of age card, passport or another document that a person may use to prove their identity. It also includes biometric information such as fingerprints, iris scans or photographs.

This Information Sheet gives compliance tips and examples for clubs and pubs when they copy, scan or otherwise collect personal information about their patrons.

For some smaller hotels, bars, clubs and other entertainment venues that are not covered by the Privacy Act this Information Sheet outlines good privacy practice.

## Key Messages

More and more clubs and pubs are using technology to electronically capture identity information about individuals. Collecting identity information in this way raises privacy concerns. There is a balance between using technology for business purposes and protecting individual privacy.

Personal information can be collected using technology by scanning or copying identity documents or capturing biometric information such as fingerprints, iris scans or photographs.

Before collecting information from their patrons, clubs and pubs covered by the Privacy Act should ask themselves:

*Is this information necessary for one of my business' functions or activities?*

If the answer is *no*, the information must not be collected. Collecting unnecessary information is a breach of the Privacy Act.

If the collection is necessary, the business must follow the NPPs when handling information.

Generally, under the Privacy Act, businesses must:

- only collect information that is necessary for their functions or activities
- tell people when they collect personal information:
    - why they are collecting information
    - what it will be used for
    - who they will pass the information onto
    - how people can gain access to it
    - any law that means the information has to be collected
    - what the consequences are if the information is not given
    - when they will destroy it
- limit the ways they use or disclose the information
- have robust security measures that protect the information
- be open about the way they handle information they collect, and
- delete the information when it is no longer necessary.

A business must also have an individual's consent before it collects health or other sensitive personal information such as organ donor status. Special rules apply to sensitive information.

Businesses that comply with the NPPs are protecting their customers' privacy and also lower the risk of privacy complaints being lodged against them.

Individuals may make a complaint to the Privacy Commissioner if they think their personal information has been mishandled. The Privacy Commissioner also has the power to initiate investigations into practices that are of concern.

## Why is scanning a privacy issue?

The Australian community has legitimate concerns about the possible misuse of personal information. People are particularly concerned about the scanning of information on

driver's licences and other proof of identity documents such as passports or proof of age cards, and when they are asked to provide their fingerprints or other biometrics.

Individuals are also worried that stored personal information could be hacked, stolen or inappropriately accessed or misused, causing harm through financial, credit card or identity fraud. Blogs about ID scanning show that individuals are concerned that they may be contacted outside of the venue by a club or pub employee who has accessed their identity information.

Electronically stored information can be copied, searched, used or disclosed more easily than in paper form and in ways that patrons may not expect. For example:

- creating customer databases
- direct marketing
- matching personal information held by other organisations which can give a detailed picture of people's day to day activities.

**Compliance Tip:**

√ Good privacy practices are good for business. Avoid privacy risks. Promote trust and confidence in your business. Don't routinely scan your patrons' ID.

## More information

The Privacy Commissioner encourages clubs and pubs to look at the following Information Sheets and guidance which give more information about scanning, the NPPs and small business obligations:

- *Information Sheet 20 - 2007 Scanning 'Proof of Identity' documents*. This Information Sheet has additional information about scanning identity documents and how the NPPs work.
- *Information Sheet 12 - 2001 Coverage of and Exemptions from the Private Sector Provisions*
- Small Business. This section of our website has information for businesses that may not be sure if they are covered by the Privacy Act.
- Guidelines to the National Privacy Principles. These Guidelines give more detail and examples about handling personal information and the NPPs.
- Frequently Asked Questions - ID scanning.

# Compliance Tips

Here are tips for clubs and pubs on using scanned identity information. They cover staff privacy training, collection, use and disclosure, data quality and storage, sensitive information, consent and meeting NPP obligations.

## Collection

Generally, under NPP 1, clubs and pubs must:

- only collect information necessary for one of its functions or activities
- collect the information lawfully and fairly
- give individuals particular information about the collection.

**Note:** If a complaint is made to the Office, a club or pub will need to be able to explain why the collection of the personal information was necessary.

### Compliance tips

√ **The information must be *necessary* for one of your business functions or activities.**

If you collect information that is not necessary, you will breach the Privacy Act.

***What function or activity will you use the identity information for?***

***Do you really need the identity information so that you can do this?***

***Are there other options which will give you the same result without collecting the personal information?***

√ **You are not allowed to collect information simply because you think it may be useful in the future.**

If you collect identify information on the off-chance it may one day become useful, it is **not** necessary.

√ **Only collect the identity information you need. Limit it to what is necessary.**

***Which bits of personal information do you actually need?***

***How will you set up your systems to avoid scanning the bits you don't need?***

***How long are you keeping the information you collect? Why?***

√ **You are not allowed to collect information simply because it is convenient.**

Identity documents contain a lot of information. You are probably collecting more information than you really need. Think about what you can do to stop this practice.

√ **Consent is needed to collect 'sensitive' information (NPP 10)**

***Driver's licences contain sensitive information. Do you have consent to collect it?***

**Example:** A photo of a person will be sensitive information under the Privacy Act if it shows the person's racial origins or their religious beliefs.

A driver's licence may include information that the holder is an organ donor. This is health information and is also sensitive information under the Privacy Act.

Consent needs to be free and informed. Make sure your patrons clearly understand that their sensitive information is being collected and what it will be used for before seeking their consent.

√ **Even if you have consent, the information still needs to be necessary before you are allowed to collect it.**

√ Consider giving your patrons an option if they don't want their ID scanned.

**Example:** your patron could sign in and you could check their driver's licence.

√ **Patrons must know that their information is being collected and what will be done with it.**

Your patrons must be given details about the collection (NPP 1.3) including:

- Your organisation's name and how you can be contacted.
- How patrons can access information you collect about them.
- Why you are collecting the information.
- Who you usually give the information to.
- Any law that says you must collect the information.

- What will happen if patrons do not give you the information.

√ This information should be in a notice in the area where scanning takes place or handed out to your patrons. Make sure the notice is easy for your patrons to see and to read.

√ Information will need to be available about the way your club or pub handles personal information if someone asks for it.

√ Scanning should not be done without the patrons' knowledge and should not be done covertly. It should be clear to all your patrons when personal information will be collected using scanning devices.

√ Devices should be visible to the patron while information is being scanned. Identity information should not be taken away and scanned in another room.

## Anonymity

Under NPP 8, patrons have the right to do business with you anonymously – without having to identify themselves – if it is practicable and lawful. This is not always possible. **Example:** Some licensing laws or laws that prevent money laundering require you to know your customer.

These laws may mean that information only has to be sighted, **not** scanned, copied or retained. If a complaint is made to the Office, a club or pub will need to be able to explain why it did not just sight a document without scanning it. In investigating complaints about anonymity the Privacy Commissioner will need to be satisfied that the business cannot function without collecting ID information.

## Compliance tips

√ You can just simply sight driver's licences or other identity documents your patrons may have to prove their age.

√ If it is lawful and practical, you do not need to scan or copy the ID. Just check that it is legitimate.

√ If lawful and practicable, let individuals deal anonymously with your organisation.

## Staff privacy training

### Compliance tips

√ **All staff that handle personal information should be privacy-trained.**

√ Staff should be able to answer patrons' questions about why your business is collecting identity information.

√ Remember to train your door-management staff in privacy as they are your front line in customer relations.

√ Staff or patrons should not feel intimidated about privacy or about asking privacy questions.

Apart from meeting your legal obligations, your patrons will feel more comfortable giving you their information if your staff can clearly explain why it is being collected and what will be done with it.

## Use and disclosure

Under NPP 2, a club or pub may only use personal information for the primary purpose for which it is collected, and in other limited circumstances. The primary purpose should be narrow and specifically defined.

NPP 2 also has rules about secondary purposes and the use and disclosure of personal information for direct marketing.

### Compliance tips

√ The reason you collected the identity information is your 'primary' purpose and you are allowed to use or disclose the information for this reason.

***Ask yourself why you are collecting the information?***

**Example:** If you collect the information for security reasons (so that you know who is in your venue at a particular point in time), then this is your 'primary' purpose.

√ **You can only use or disclose the information for another purpose (a 'secondary' purpose) if it is allowed under NPP 2.1.**

If none of the exceptions under NPP 2.1 let you use or disclose the information for a secondary purpose, you **cannot** do it.

√ **To use the information for the secondary purpose of direct marketing, you must comply with NPP 2.1(c).**

√ You must give the person the choice to opt-out of receiving future marketing material.

## Consent

Consent should be informed and freely given. Patrons should have a clear understanding of what information is going to be collected, why, how the information will be used and who the information is usually given to.

**Remember: Sensitive information is given a higher level of protection under the Privacy Act**.

Generally, seeking consent from your patrons may give you greater confidence about the way you are meeting your obligations under the Privacy Act. Seeking consent is not just good privacy practice, it helps to promote trust between the patron and your club or pub.

**More information**

- Guidelines on Privacy in the Private Health Sector

## Data quality

### Compliance tips

√ **The information you have scanned and stored must be accurate, complete and up-to-date.**

How old or how reliable is the information you are collecting, using or disclosing? If it is old, it may no longer be accurate and you may need to check it. Relying on information that is incorrect or out-of-date is not good for your business reputation. Under NPP 3, you must take reasonable steps to make sure information is accurate complete and up-to-date before it is collected, used or disclosed.

## Data security

Under NPP 4, clubs and pubs must take reasonable steps to protect the personal information they hold. Scanned personal information is vulnerable as the personal information can be used to prove identity in other situations. **Example:** to open bank accounts, get credit, or prove identity for some government services.

Under NPP 4.2, reasonable steps must be taken to destroy or permanently de-identify personal information when it is no longer needed.

**Example:** Scanned personal information is collected to ensure the safety and security of a club's premises and patrons. If no incident occurred on the date of collection, or is reported soon after, the club will probably not need to keep that personal information after that date.

### Compliance tips

√ **Have a security policy that reduces privacy risks in your pub or club to acceptable levels.**

Think about internal **and** external threats to privacy. There are risks to the individual (identity fraud) and risks to your business (loss of data, loss of reputation, payment of compensation) if there is a security breach.

√ **Store electronic identity information securely.**

- Limit staff access.
- Have a stand-alone terminal that isn't networked and not able to be used with portable storage devices.
- Don't have a group password.
- Have audit trails so you can see who has accessed the information.
- Train your staff.
- Have physical measures in place, like locked offices.

√ **Set strict timeframes for keeping identity information.**

Have a policy in place that sets time frames for how long you keep the personal information you have collected. Regularly check if you still need the identity information. If you don't need it, destroy it securely.

√ **Staff should understand how important it is to keep personal information secure.**

√ **Staff should be able to explain to customers how your business keeps their information secure and why.**

Remember, your staff are your front line in privacy security. Make sure they understand their privacy responsibilities. **Training! Training! Training**!

## Openness

Under NPP 5, clubs and pubs may need to give people more details about how their personal information is handled. You must also put this information in a privacy policy and make it available to anyone who asks.

A privacy policy should describe:

- what scanned and other personal information the club or pub collects
- how the information is collected using scanning devices
- why the club or pub has collected it
- how the club or pub stores, uses and discloses that personal information
- the IT security measures to protect the electronically stored information
- how long the information is kept for
- how the information is destroyed.

A club or pub can also give these details to individuals when collecting the information.

## Compliance tips

√ **Your privacy policy must clearly set out how your organisation handles privacy and personal information.**

Include information about the kinds of personal information you hold, the purpose, how you can be contacted, how to get more information about the policy or how to make a privacy complaint.

√ **Your privacy policy must be readily available.**

Have your policy available electronically and in hard copy for anyone who requests it.

## Identifiers

Many identification documents carry what is known as an 'identifier'. **Example:** a passport number.

**Organisations must not use or disclose identifiers issued by Australian Government agencies, such as Tax File, Medicare or Passport numbers, except in prescribed circumstances.**

### Compliance tip

√ Don't collect Australian Government identifiers. This means not collecting, scanning or copying identifiers such as Australian passport or Medicare numbers.

## Scanning and contractors

A club or pub may contract out the scanning of customers' identity documents.

If the contractor is covered by the Privacy Act, then it will have the same privacy obligations as described above. A contractor may also come under coverage because it handles personal information for a benefit, service or advantage.

To make sure personal information is not mishandled, a club or pub could ask the contractor to opt-in to coverage or to make opting-in a term of the contract.

**More information**

- Information Sheet 8 - 2001 Contractors
- Opt-in Register

## About Information Sheets

Information sheets are advisory only and are not legally binding. The National Privacy Principles (NPPs) in Schedule 3 of the Privacy Act 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 freedom 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 30

Web HTML and PDF published May 2010

ISBN 978-1-877079-65-8



**www.privacy.gov.au**