

ID SCANNING **privacy responsibilities** **FOR LICENSED VENUE STAFF**

Information notes



This document is to be used in conjunction with the [ID scanning privacy responsibilities for licensed venue staff sample presentation \(PPT\)](#).

NOTE 1 - SLIDE 2 and 3

- The implementation of the networked ID scanner scheme contributes to the Queensland Government's Tackling Alcohol Fuelled-Violence reforms.
- Networked ID scanning is an effective mechanism to support the enforcement of patron bans, helping to keep Queenslanders safe by minimising the risk of alcohol-related harm.
- Non-exempt licensees in safe night precincts who trade past midnight on a permanent basis are obliged to install an approved ID scanner at each entry to the licensed premises.
- These licensees are referred to as 'regulated premises' under the ID scanner scheme.
- This document explains staff's privacy obligations as an employee of a regulated premises.
- Under the *Liquor Act 1992*, licensees and staff of regulated premises must comply with the privacy requirements of the *Privacy Act 1988* (Cth).
- The privacy laws include **13 Australian Privacy Principles** to safeguard and protect the handling of personal information.
- As an employee of a regulated premises, you have privacy obligations when operating and accessing information collected by ID scanners.

NOTE 2 - SLIDE 4

Why are privacy laws important?

ID scanners collect personal information from patrons in the form of a photograph, name and date of birth. It is important that staff understand their role in protecting this personal information from misuse, loss and unauthorised access.

Why is privacy training important?

It is important that staff are able to answer questions from patrons who may be concerned that the personal information collected about them by the ID scanners could be shared, stolen or misused.

It is also important that staff understand their obligations about protecting personal information.

NOTE 3 - SLIDE 5

Australian Privacy Principles

There are 13 Australian Privacy Principles (APPs) that a venue must adhere to when collecting personal information:

- **Principle 1 - Open and transparent management of personal information**
- **Principle 3 - Collection of solicited personal information**
- **Principle 5 - Notification of the collection of personal information**
- **Principle 6 - Use or disclosure of personal information**
- **Principle 7 - Direct marketing**
- **Principle 10 - Quality of personal information**
- **Principle 11 - Security of personal information**
- **Principle 12 - Access to personal information**
- **Principle 13 - Correction of personal information**

Note: APPs 10, 12 and 13 are particularly important and will be explained in more detail in the following slides.

NOTE 4 - SLIDE 6

Privacy Principle 1 – Open and transparent management of personal information

The venue is required to manage personal information in an open and transparent way. The publicly available *Privacy Policy* should detail how staff are to manage personal information in this manner.

How does this principle apply to Licensees and staff

Licensee are to put policies into place that ensure the correct management of personal information in a transparent and open way. Take reasonable steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs.

This could mean implementing governance mechanisms, regular staff training and a program of proactive review and audit of the adequacy and currency of the venues practices, procedures and systems. The Office of the Australian Information Commissioner (OAIC) has developed a Privacy Management framework to assist in the development and review of the venues privacy program. Available at <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework>.

The OAIC have a Guide to Developing an APP Privacy Policy, which provides some tips and sets out a process for developing a privacy policy, as well as useful checklist. The most important thing is to make sure the privacy policy is easy to read and understand.

NOTE 5 - SLIDE 7

Privacy Principle 3 – Collection of personal and sensitive information

ID scanners collect personal information. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable (whether or not the information or opinion is true and whether or not it is recorded).

The personal information collected by the ID scanner is limited to:

- Name
- DOB
- Photograph

The venue is permitted to collect personal information because it relates directly to the purpose of the ID scanner scheme i.e. to be able to more easily identify if a person is subject to a police, court or licensee ban.

Certain de-identified data may be accessed by the Government. Patrons should be advised to contact OLGR for further information.

How does this principle apply to licensees and staff?

When scanning patrons ID, it is important that staff correctly handle their personal and sensitive information. For example, it is not appropriate for licensees or staff to record a patrons details for personal use (such as contacting the patron) or to share a patron's ID with other staff members.

If the ID scanning system has failed and the venue is using a 'manual list' to check patron's ID staff need to be aware that the list contains personal and sensitive information about persons subject to a court or QPS banning order or a licensee ban. As such, staff must be careful where the list is stored and who it is shown to etc. For example, the list should not be able to be viewed by patrons entering the venue.

Collection must be 'reasonably necessary' for one or more of an APP entity's functions or activities:

- the personal information captured by the ID scanner will include name, date of birth and photo
- de-identified data will be accessible by OLGR for statistical purposes and to evaluate the success of the ID scanner scheme (this information will be limited to premises name, number of people who entered the premises on a given night, positive ban check etc.)
- personal information must not be collected unless it is reasonably necessary for one or more of the venues functions/activities.

NOTE 6 - SLIDE 8

Privacy Principle 5 – Notification of collection

Regulated premises are required to notify patrons that approved ID scanning systems operating at the premises will collect personal information. This is to be done by displaying a *Collection Notice* at each public entrance to the premises.

How does this principle apply to licensees and staff?

Reasonable steps must be taken to notify the individual about these matters when collecting personal information, regardless of who the information has been collected from. So, if individual's personal information has been collected from another business, reasonable steps will still be needed to make sure the individual is aware of the relevant matters

Under the Privacy Act, regulated premises must notify patrons of ID scanner requirements prior to having their photo ID scanned and must display these **collection notices (Licensee to include image of collection notice and its location on the premises)** at each public entrance to the regulated premises. A sample collection notice is available at www.business.qld.gov.au/id-scanning. This document has been prepared by The Office of Liquor and Gaming Regulation as a guide.

Includes:

- who the entity is and how to contact it
- the purpose(s) of the collection
- usual disclosures to third parties
- complaint handling process
- likely overseas disclosure.

NOTE 7 - SLIDE 9

Privacy Principle 6 – Use or disclosure

Information collected by ID scanners used for the purpose of identifying if a person is banned from a licensed premises. With the exception of responding to a lawful request from a law enforcement agency it should not to be disclosed for any other purpose.

There might be circumstances where {insert venue or licensee name} would want to use or disclose the information for a secondary purpose, without necessarily obtaining consent. Following are some examples:

- if the individual would reasonably expect the venue/staff to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose if the use or disclosure is necessary to assist in the location of a person reported as missing

- if the venue/staff have reason to suspect that unlawful activity or serious misconduct relating to the venues functions or activities may be being engaged in, and the use or disclosure is necessary for you to take appropriate action
- if the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

NOTE 8 - SLIDE 10

Privacy Principle 7 – Direct Marketing

(only include if this applies to your venue)

A licensee of a regulated premises may only use personal information for the primary purpose for which it is collected (i.e. identifying banned patrons), and in other limited circumstances as outlined in section 7.2 of the APPs.

Section 7.2 provides that a regulated premises may use or disclose personal information about a patron for the purpose of direct marketing.

OLGR is aware that approved operators may offer value-added services to enhance the capability of their approved ID scanner. If your venue decides to use personal information collected for other purposes, such as direct marketing, patrons need to know that it is being collected for this purpose and be able to correct the information and/or opt out.

Licensees and staff are required to make patrons aware of their intentions for use of personal information through displaying notices at all entries to the venue and must also make patrons aware of how they can easily request not to receive direct marketing communications.

Approved Operators may offer licensees of regulated premises value-added services to enhance the capability of their approved ID scanner. Before a licensee signs up for value-added services they should consider whether the service complies with the APPs and their obligations under the Privacy Act.

How does this principle apply to Licensees and staff?

Can the licensee use or disclose personal information for direct marketing?

You can do this if the licensee collected information from an individual and that individual would reasonably expect the licensee to use or disclose the information for direct marketing purposes. However, where the individual wouldn't reasonably expect the licensee to use or disclose the information for that purpose, or the licensee collected the information from a third party, then the licensee would generally need to get the consent of the individual.

In each of these scenarios the licensee will be required to provide a **'simple means'** for the individual to opt-out of receiving any marketing. You must also generally include a **'prominent statement'** informing the individual of the option to make such a request. Staff need to be made aware of the 'opt-out' venue procedure.

NOTE 9 - SLIDE 11

Privacy Principle 10 – Quality

- Licensed venues/licensees must take reasonable steps to ensure personal information it collects, uses or discloses is accurate, up-to-date, complete and relevant.

- Must also take reasonable steps to ensure that personal information is relevant for the purpose of the use or disclosure. Acceptable ID includes:
 - all Australian driver's licences
 - all adult Proof of Age cards and interstate equivalents
 - Australian and Foreign Passports
 - Australia Post Keypass identity card
 and
 - Foreign driver's licences (which must display name, photo and date of birth of the licence holder). Where a foreign drivers licence is not in English, an international driver permit issued in the foreign country of origin.

NOTE 10 - SLIDE 12

Privacy Principle 11 – Security

The approved ID scanning system will automatically delete scanned personal information after **30 days**.

Access to scanned data (including personal information) at a regulated premises will be restricted to a limited number of people, such as venue management.

Licensees and staff are required to provide access to patron scan data from your approved ID scanner upon request from an enforcement body.

This access will be auditable as the approved ID scanning system will retain a record of the login details of all persons who log on to the approved ID scanning system at the premises. Some best practice measures that you may take to meet your obligations would be:

- limiting staff access to the approved ID scanning equipment
- not having a group password
- staff training
- physical measures to keep approved ID scanning equipment secure, including locking offices and ensuring the equipment is constantly supervised.

How does this principle apply to licensees and staff

Here a venue could outline the steps they take to ensure the security of the personal information they collect (see access to personal information section of ID scanner guide).

Licensee to detail what measures they employ for the retention for banned and scanned data, who has access to it, who can modify it and who it can be disclosed to.

NOTE 11 - SLIDE 13

Privacy Principle 12 – Access to personal information

A person has the right to access personal information held about them by a licensee. Some exceptions apply, such as where access would be likely to interfere with criminal matters, or other breaches of the law.

NOTE 12 - SLIDE 14

Privacy Principle 13 – Correction of personal information

A person is able to request the personal information held about them be corrected. For personal information to be corrected, satisfactory proof or explanation as to why the information needs to be corrected would be required.

NOTE 13 - SLIDE 15

How to deal with patron complaints

Staff have an obligation to inform patrons about how they can make a privacy complaint.

Information on how a person can make a complaint must be advertised on the **collection notice** which is required to be displayed at or near any public entrance to a regulated premises, as well as detailed in the venue's **privacy policy**.

Steps for regulated premises to deal with a privacy complaint:

1. Accept and review written privacy complaints.
2. Notify the OLGR that a written privacy complaint has been received within 14 days of receiving the complaint. This can be done by logging in to the OLGR client portal and selecting the form titled Privacy Complaint.
3. Provide a response to the person's privacy complaint within 30 days.
4. If the person is not happy with the outcome, provide the person with details on how to lodge a complaint with the OAIC. Refer the person to the regulated premises' collection notice and privacy policy.

NOTE 14 - SLIDE 16

Measures taken by (venues/licensee name) to protect personal information

Examples:

- We have a ('[privacy management plan](#)') about how we handle privacy issues (*attach copy of the venue's privacy management plan*).
- We make our '[privacy policy](#)' publicly available (free-of-charge) detailing how we manage personal information obtained from ID scanning (*attach copy of the venue's privacy policy*).
- We display a '[collection notice](#)' at or near the entrance to the venue, (*attach copy of the venue's collection notice*).
- We only operate approved [ID scanners and systems](#).
- We only collect information for the purpose of checking that a person isn't banned from the premises.
- We review all privacy complaints received and respond within 30 days and notify OLGR within 14 days.
- Our staff receive privacy training so they can answer questions from the public and understand their obligations regarding protecting personal information.

NOTE 15 - SLIDE 17

Useful resources for licensees

- Further information on how venues can comply with their privacy obligations are available on the website of the Office of the Australian Information Commissioner <https://www.oaic.gov.au/privacy-law/rights-and-responsibilities>.
- OAIC's Privacy Management Framework at <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework>.