Gambling Administration Guidelines

Facial Recognition System Requirements

Effective 3 December 2020

The following facial recognition system requirements have been published by the Liquor and Gambling Commissioner under section 17 of the *Gambling Administration Act* 2019 for the purposes of section 40D of the *Gaming Machines Act 1992* and section 40D of the *Casino Act 1997.*

1. Introduction

Under section 40D of the *Gaming Machines Act 1992* and section 40D of the *Casino Act 1997*, the Liquor & Gambling Commissioner (the Commissioner) may approve a system to be operated by certain licensees that enables the facial image of a person who is entering a gaming area to be recognised, identified and recorded (***a facial recognition system***).

The Commissioner must not approve a facial recognition system unless the system complies with any requirements prescribed by the Gaming Machines Regulations 2020 and Casino Regulations 2013, and from 3 December 2020, is able to be operated in accordance with any Gambling Administration Guidelines issued by the Commissioner under section 17 of the *Gambling Administration Act 2019.*

2. Commencement

These guidelines come into effect from 3 December 2020, being the date determined by the Commissioner by notice published in the South Australian Government Gazette.

The Commissioner may by notice in the Gazette vary or revoke these guidelines at any time in accordance with section 17(3) of the *Gambling Administration Act 2019*.

Version control will be used to indicate revisions to these guidelines.

3. Intended Audience

These guidelines are intended for use by facial recognition technology providers for the evaluation of facial recognition systems submitted to the Commissioner for approval for use in South Australia.

4. Purpose and scope

(1) The purpose of these guidelines is to ensure that approved facial recognition systems operate in South Australia to identify barred persons entering a gaming area must:

(a) accurately take account of physical variances in facial features;

(b) prevent unauthorised access, use and disclosure of data collected by the system; and

(c) operate in accordance with any technical requirements, security requirements and any other criteria as determined by the Commissioner.

(2) It is not the purpose of these guidelines to mandate a solution or limit technology.

(3) Any matters arising from the evaluation of a facial recognition system not covered by these guidelines will be considered for approval at the discretion of the Commissioner.

5. Interpretation

(1) In these guidelines, unless the contrary appears—

(a) ***facial recognition system*** means a biometric technology capable of identifying or verifying a natural person using a digital image or a video frame captured from a fixed video source;

(b) ***gambling provider*** means:

i. the holder of a gaming machine licence under the *Gaming Machines Act 1992*; and

ii. the holder of the casino licence under the *Casino Act 1997*.

(c) ***facial recognition technology provider*** (system provider) means:

i. an entity which administers a facial recognition system, approved by the Commissioner for the purposes of the *Gaming Machines Act 1992* or *Casino Act 1997*; and

ii. who has entered into a contract or agreement with a gambling provider to provide an approved facial recognition system; and

iii. who is a party to an executed Data Sharing Agreement with the Commissioner; and

iv. who is approved by the Commissioner.

6. Submissions general

(1) Facial recognition technology providers seeking approval for the deployment and use of facial recognition systems in Hotels and Clubs in South Australia and the Adelaide Casino, must submit an application seeking approval of the system to Consumer and Business Services (CBS).

(2) Facial recognition technology providers seeking approval for the deployment and use of facial recognition systems at the Adelaide Casino must also satisfy the Commissioner that the system submitted for approval has been selected by the casino licensee as suitable for deployment at the Adelaide Casino.

(3) Applications must be made in the manner and form approved by the Commissioner and be accompanied by the prescribed fee.

(4) Applications must contain at least the following elements:

(a) the date of the submission;

(b) the full name of the system provider, address for service, address of the principal place of business;

(c) a declaration by the person/s responsible for the submission that the information submitted is true and correct;

(d) the details of where technical enquires regarding the submission may be directed;

(e) the registered business identification number and address of the entity (for example an ABN if registered in Australia or NZBN if registered in New Zealand);

(f) a company extract supported by written text explaining the corporate structure of the entity, in particular in relation to parent or holding companies, subsidiaries, other associated companies, directors and major shareholders;

(g) the details of—

A. any licence or approval applied for or held by the entity, or a holding, parent or subsidiary company of the entity, for the approval and deployment of facial recognition technology in any other State, a Territory of the Commonwealth or New Zealand; and

B. any refusal to grant or renew any such licence or approval; and

C. any suspension, cancellation or revocation of, or other disciplinary action in respect of, any such licence or approval; and

D. details of a where the solution is currently in operation;

(h) the details of the system providers technical expertise in the deployment of facial recognition technology;

(i) a description of the product being submitted and the intent of the submission;

(j) system architecture diagram and description on how the facial recognition system is intended to be operated within a business;

(k) details of the facial recognition algorithm(s) and associated independent testing data;

(l) a copy of the data breach response plan including safeguards or controls within the system to guard against misuse, unauthorised access or sharing of information; and

(m) details of any independent penetration testing of the system, particularly in relation to the security of stored barred person data.

(5) A system provider must also enter into a Data Sharing Agreement with the Commissioner to facilitate the exchange of information between the parties for the proper administration of relevant laws and policies.

(6) Any test reports provided in support of an application must contain the testing body's name, accreditation details, the name of the individual who conducted the testing, a description of what was tested, how it was tested (photos may be required) and the test results.

(7) All submission documentation and electronic media must be labelled with the company name, the product name, the product version and the submission date. Resubmissions must also include the resubmission number (e.g. version 2). Version numbers are to be unique and any change to an already approved submission should require this unique version number to change.

(8) As part of the assessment process the Commissioner may request a demonstration of the system to assist in making a determination.

(9) Any enhancements or changes to an approved system prior to production deployment must be notified and approved by the Commissioner before deployment.

(10) The approval of a facial recognition system for these purposes may be varied or revoked by the Commissioner in accordance with section 40D of the Casino Act *1997* and section 40D of the *Gaming Machines Act 1992*.

7. Software submissions

(1) All submissions must be in English.

(2) Submissions must include a list of all known unresolved issues, bugs and incidents. This list must be comprehensive and include any issues identified with previous versions which have not been resolved with the current version, even if these issues have been previously notified to CBS.

8. Hardware Submissions

(1) Submissions must include all relevant technical details, specifications and datasheets pertaining to all components of the facial recognition system (including video capturing devices, CPU, system backend, etc.).

(2) Submissions must include the details of any specific hardware to be operated in connection with the solution (including off the shelf or proprietary hardware).

9. General Requirements

(1) Facial recognition technology is one of many biometric technologies that can be used to identify a natural person.

(2) A facial recognition system for the purposes of these guidelines must be capable of identifying or verifying the physical features of a natural person's face using a digital image captured from a fixed video source.

(3) A facial recognition system will generally consist of:

(a) one or more fixed video capturing devices;

(b) one or more CPU running proprietary software, including complex algorithm(s), that identify and compare points or surfaces of a person's face and features;

(c) a graphical user interface (GUI) to view and manage the capturing of images for the purpose of identification; and

(d) can be hosted on-premises, in the cloud or a hybrid on-premises and cloud-based host.

10. Requirements under the *Gaming Machines Act 1992*

(1) This part applies to the operation of facial recognition technology **by the holder of a gaming machine licence** for the purposes of the *Gaming Machines Act 1992*.

(2) As of 3 December 2020, a licence holder (licensee) must for the purposes of identifying barred persons entering a gaming area, operate a facial recognition system if the gaming machine licence for the premises authorises the operation of thirty (30) or more gaming machines (being a reference to the number of gaming machine entitlements affixed to a licence) any one (1) of which may be operated by the insertion of a banknote.

(3) A licensee not subject to the above licence condition may deploy facial recognition technology to support their responsible gambling obligations.

(4) A licensee must only use a facial recognition system approved by the Commissioner for this purpose.

(5) A licensee should contact an approved facial recognition system provider to discuss venue requirements and negotiate terms. A list of approved system providers will be maintained on the CBS website.

(6) Once a provider is selected, the licensee must enter into a formal agreement by completing the **Confirmation of Engagement of an Approved FRT Provider by a Licensee** form, which is available on the CBS website, and submitting this form to CBS. On receipt, the selected FRT provider will be granted access to the barring data of the relevant licensed premises.

(7) The licensee will be responsible for providing CBS with copies of any updated agreements during the engagement period.

(8) A licensee must ensure that an approved facial recognition system is always in operation when gaming machines are able to be operated on the licensed premises.

(9) Data collected by a facial recognition system operated by a licensee must not be used for or in connection with the following:

(a) encouraging or providing incentives to a person to gamble;

(b) customer loyalty programs;

(c) a lottery within the meaning of the *Lotteries Act 2019*;

(d) identifying a barred person in respect of premises other than the licensed premises in relation to which the system is operating;

(e) any other purpose notified by the Commissioner to the system provider or licence holder.

(10) Facial images or any data recorded by the approved facial recognition system that identifies a person (other than a barred person) for these purposes, must not be retained by the licensee or on the facial recognition system operated on behalf of the licensee after 72 hours of being recorded by the system.

11. Requirements under the Casino Act 1997

(1) This part applies to the operation of facial recognition technology **by the holder of the casino licence** for purposes of the *Casino Act 1997*.

(2) As of 3 December 2020, the holder of the casino licence (casino licensee) must, for the purposes of identifying barred persons entering a gaming area, operate a facial recognition system approved by the Commissioner.

(3) The casino licensee must ensure that an approved facial recognition system is always in operation when gaming operations are able to be conducted on the licensed premises.

(4) Data collected by a facial recognition system operated by the casino licensee for these purposes must not be used for or in connection with the following:

(a) encouraging or providing incentives to a person to gamble;

(b) customer loyalty programs;

(c) a lottery within the meaning of the Lotteries Act 2019;

(d) identifying a barred person in respect of premises other than the casino premises;

(e) any other purpose notified by the Commissioner to the system provider or licence holder.

(5) Facial images or any data recorded by the facial recognition system that identifies a person (other than a barred person), must not be retained by the casino licensee or on the facial recognition system operated on behalf of the casino licensee after 72 hours of being recorded by the system.

(6) Notwithstanding this part, a security and surveillance system approved by the Commissioner for the purposes of section 38 of the Casino Act 1997 may retain the facial images of persons entering and remaining on the casino premises to:

(a) safeguard the licensee's assets;

(b) protect both the public and licensee's employees; and

(c) promote public confidence that licensed gambling activities are conducted honestly and free of criminal elements and activities.

12. Facial Recognition Technology – Provider Requirements

(1) A facial recognition system operated by a gambling provider that enables the facial image of a person when entering a gaming area to be recognised, identified and recorded for the purposes of *Casino Act 1997* or *Gaming Machines Act 1992* must be approved by the Commissioner before a facial recognition system provider (system provider) can be engaged to provide such services by a gambling provider.

(2) Data disseminated, collected or exchanged with a system provider for these purposes must be stored on-shore and cannot be exported off-shore or used in other applications.

(3) A system provider must produce evidence of engagement with a gambling provider before access to any barring data will be granted. Any changes to the use of this data or contracted period of engagement with a gambling provider must be approved by the Commissioner.

(4) A system provider must not disclose or share any information or data about barred persons collected by an approved system other than to the South Australian gambling provider who has engaged the services of the system provider or the Commissioner.

(5) A system provider must, in the form and manner determined by the Commissioner, advise the gambling provider and the Commissioner of any unplanned outages that have impacted on the ability of an approved system to identify barred persons.

(6) A system provider must make all reasonable efforts to repair any malfunction of an approved system as soon as practicable after the malfunction is discovered.

(7) As soon as the gambling provider or system provider becomes aware that a video capture device, software or GUI has malfunctioned, reasonable steps must be taken to have the video capture device, software or GUI repaired, replaced or take such other measures to protect the subject activity. For example, additional employee monitoring of the gaming area.

(8) Scheduled maintenance of an approved facial recognition system, including any video capture device, software or GUI must be planned and undertaken at a time of day where the risk of a barred person being able to gain entry to a gaming area is minimised.

(9) A system provider must within 7 days of becoming a party to any other Facial Verification or Matching System granted by the Commonwealth of Australia notify the Commissioner of that engagement.

13. Facial Recognition Technology – System Requirements

(1) The system must be able to make multiple '**GET'** requests via a secure webservice with an authentication header for each request.

(2) The system solution must be able to utilise '**Hypertext Transfer Protocol Secure'** (HTTPS).

(3) The system must be able to '**CONSUME**' barred person data, returned in JavaScript Object Notation (JSON) format, that includes the following data:

- (a) Venue name
- (b) Venue ID
- (c) Licensee name
- (d) Barred patron details
  - i. Given name
  - ii. Family name
  - iii. Full name
  - iv. Date barred from
  - v. Date barred to
  - vi. Images
    - A. Identification reference
    - B. Name
    - C. Extension
    - D. Image content

(4) The system must be able to purge all data related to a barred person once a barring is revoked or no longer active.

(5) The system must be able to record the date and time of day that a person identified by the system as a barred person was first:

- (a) detected entering a gaming area by the system; and
- (b) approached in-person by an authorised employee of the gambling provider for the purpose of identity confirmation.

(6) Notwithstanding the requirements of this part, a security and surveillance system approved by the Commissioner for the purposes of section 38 of the *Casino Act 1997* may be used by the casino licensee to record the information for this purpose.

(7) The system must be able to '**POST**' usage data to the CBS Host using a secure webservice on a daily basis, providing as a minimum the following data:

(a) Venue ID

(b) Venue Name

(c) Number of faces identified in that day

(d) Number of barred persons identified in that day

(e) Time taken (recorded in milliseconds) between detection by the system of a suspect barred person and first contact acknowledged

(f) Incidents of system downtime.

(8) The system must ensure that facial images, barred person data, or usage data, is protected by access authentication control and is encrypted when at rest and in transit.

(9) Notwithstanding the requirements of this part, a security and surveillance system approved by the Commissioner for the purposes of section 38 of the Casino Act 1997 may be used by the casino licensee to '**POST**' usage data to the CBS Host for this purpose.

(10) The system must have the ability to send non-identifiable '**PUSH**' notifications to a secure device by email, SMS or both, to an authorised employee of the gambling provider who is on duty or is responsible for a gaming area, for the purpose of making them aware a barred person is entering the gaming area.

(11) Notwithstanding the requirements of this part, a security and surveillance system approved by the Commissioner for the purposes of section 38 of the *Casino Act 1997* may be used by the casino licensee to notify an authorised employee of the casino licensee who is on duty or is responsible for controlling entry to the casino premises, for the purpose of making them aware a barred person is entering the casino premises.

(12) The system must purge all data relating to the facial images of persons who have entered the gaming area within 72 hours of detection.

14. References

Gambling Administration Act 2019

Gaming Machines Act 1992

Gaming Machine Regulations 2020

Casino Act 1997

Casino Regulations 2013

15. Revision History

Version	Changes	Release Date
1	Original document published as notified technical requirements	27 July 2020
2	Original document updated to include further definitions	15 October 2020
3	System requirements re-issued as Gambling Administration Guidelines for the purposes of the *Gambling Administration Act 2019*	3 December 2020