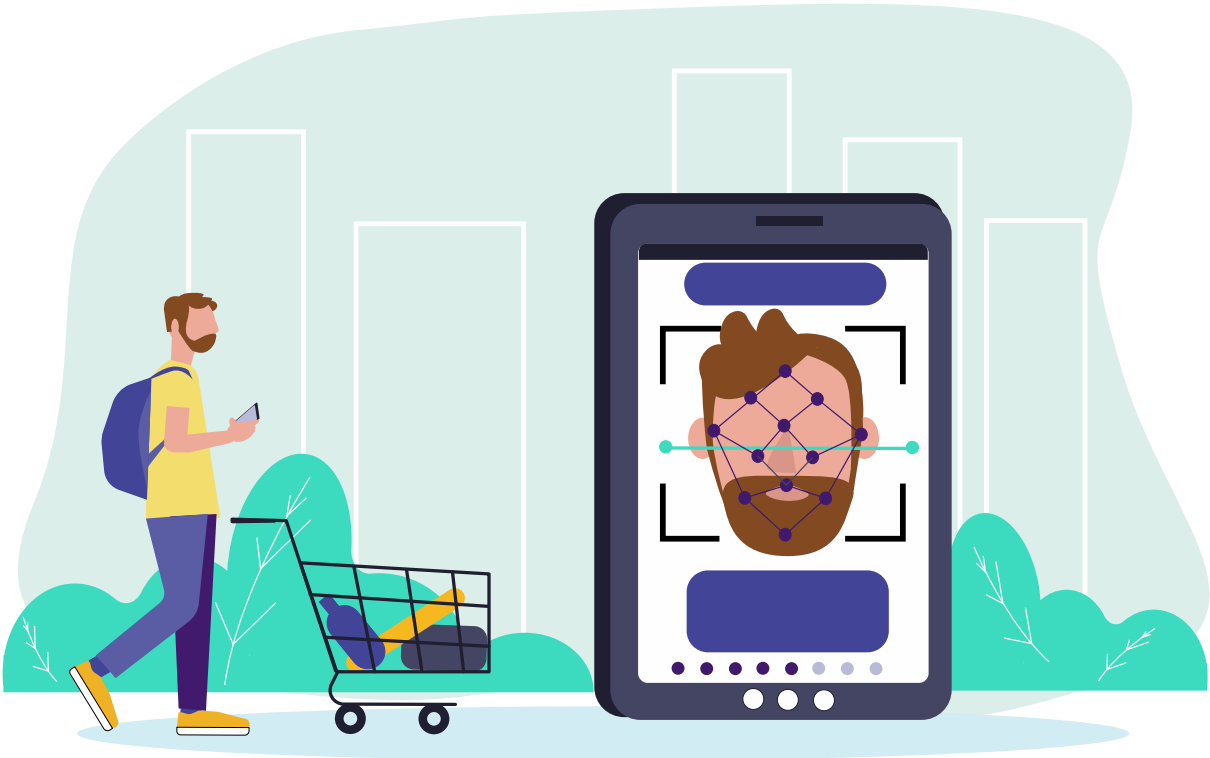
Privacy essentials checklist for considering facial recognition in physical settings (such as retail)

This checklist is intended to help entities considering using facial recognition technology (FRT) in physical settings which are open for the public to freely move through, such as a retail shopfront.

The checklist is a tool to assist entities to consider the lawfulness of deploying FRT and the essential privacy obligations that apply when collecting personal and sensitive information using FRT. It does not cover the entirety of privacy obligations under the Australian Privacy Principles. This resource should be read in conjunction with the [OAIC's Privacy Guidance for Facial Recognition], as well as the *Privacy Act 1988* (Cth), the Australian Privacy Principles guidelines (APP guidelines), and other OAIC resources referred to in this checklist.



Question 1

Have you conducted a detailed risk assessment about using FRT, including a privacy impact assessment?

Entities considering using FRT should conduct a detailed risk assessment before implementing the technology.

A privacy impact assessment (PIA) provides a structured way to identify potential privacy impacts at the outset and, if proceeding with FRT, implement recommendations to manage, minimise or eliminate those impacts.

Completing a PIA will help you to navigate the questions and processes contained in this checklist.

For Commonwealth agencies, conducting a PIA is a requirement for all high privacy risk projects.

See Part A of the guidance.

Additional resources

Guide to undertaking privacy impact assessments

Privacy impact assessment tool

Privacy by design

Question 2

Is there a lawful basis under APP 3 for collection of sensitive information via FRT?

FRT systems collect the sensitive information of every person whose face is captured, even if they are not a 'match'. Entities may only collect sensitive information with the consent of each individual, unless an exception pathway applies.

Relevant exception pathways include:

- Where specifically authorised or required by law or a legal order.
- Where a Permitted General Situation relating to serious threats and unlawful misconduct exists.

In considering if a permitted general situation applies, consider whether using FRT is reasonably necessary, by assessing:

- the **suitability** of collecting sensitive information in your situation,
- the **alternatives** that are available, and
- whether the privacy impact is **proportionate** to the benefits of collection.

If you have concluded after conducting this assessment you have formed a reasonable belief that an exception or Permitted General Situation exists, ensure that you comply with your ongoing Privacy Act obligations in relation to the deployment of FRT in your business (see factors below).

See Part B of the guidance.

Additional resources

APP Guidelines Chapter 3: Collection of solicited personal information
APP Guidelines Chapter C: Permitted general situations
Facial recognition technology: a guide to assessing the privacy risks

Question 3

Do you have a clearly expressed and up to date privacy policy explaining how you collect and manage personal information?

Have a privacy policy that describes in plain English what personal information you collect, how you collect that information, and how and why you use that information.

Identify the updates that are needed to your privacy policy in order to explain how you collect and manage personal and sensitive information using FRT, including biometric information and biometric templates.

See Part A of the guidance.

Additional resources

Guide to developing an APP privacy policy

Supporting poster

APP Guidelines Chapter 1: Open and transparent management of personal information

Question 4

Have you identified the reasonable steps you will take to notify or ensure individuals are aware of matters relating to collection of their personal information by or for FRT?

Make sure individuals are clearly informed that their information is being collected for processing using FRT, and the reason you are doing so. You need to do this even if you are not seeking individuals' consent to collect their information (i.e. on the basis of an exception pathway).

Consider what steps are reasonable in your circumstances for each of the matters listed in APP 5.2, for each collection of personal information. This includes when collecting a person's face to identify if they are a match, as well as when collecting personal information to 'enrol' someone in a database in order to later identify them.

The steps that are reasonable for each matter do not have to be identical, but generally you should provide notice to individuals which is explicit about your collection of sensitive information by use of FRT, the purpose of collection, and the consequences of opting out.

The steps you take should be designed to make individuals aware of these matters at or before the time when their sensitive information is collected or, if this is not practicable, as soon as practicable after.

See Part C of the guidance.

Additional resources

APP Guidelines Chapter 5: Notification of the collection of personal information

Question 5

Have you taken steps to ensure the biometric information that will be used by FRT is accurate, and identified any steps that need to be taken to address the risk of bias?

Entities have a responsibility to ensure information they collect is accurate, up-to-date, and complete.

Accuracy: there is a particular risk of inbuilt bias when using FRT. Unaddressed bias can lead to collection of incorrect information, which has consequences including both false positives (a 'false alarm') and false negatives (a 'missed detection').

Identify the reasonable steps you will take to ensure information you collect is accurate, and address the risk of bias in your FRT system. This extends to the risk of error or bias in the list of individuals you 'enrol' for matching in a database.

See Part D of the guidance.

Additional resources

APP Guidelines Chapter 10: Quality of personal information

Question 6

Do you have a plan to protect personal information you collect via FRT, even if you only intend to hold it briefly?

Consider the information that your FRT system will collect. Information is 'collected' by FRT when you store it in an electronic device (such as a server's RAM or hard drive), even if you intend to quickly delete it within milliseconds.

What are the reasonable steps you will take to protect this information from misuse, interference and loss, and unauthorised access, modification or disclosure?

Reasonable steps you take should include both technical and organisational measures. If your FRT system is operated by a third-party vendor, do your due diligence and ensure they are bound by appropriate contractual provisions covering security and retention. Contractual arrangements should also include mechanisms to ensure privacy obligations are being fulfilled (e.g. review and audit clauses).

See Part E of the guidance.

Additional resources

Guide to securing personal information

APP Guidelines Chapter 11: Security of personal information

Question 7

Do you have processes to ensure information you collect is destroyed or de-identified when it is no longer needed?

You need to take steps to destroy or de-identify personal information that you have collected and which you no longer require for a valid purpose under the APPs.

Implement processes that will enable you to identify when information collected via FRT is no longer needed (e.g. once you have determined the face is not a 'match') and ensure timely destruction or de-identification. Processes for data destruction should account for both personal information collected in the operation of the FRT system, and personal information collected to create the reference database of individuals the system is used to identify.

See Part E of the guidance.

Additional resources

De-identification and the Privacy Act

APP Guidelines Chapter 11: Security of personal information

Question 8

Does your organisation have clear governance arrangements in place in relation to your management of information, and your use of FRT?

Your privacy risk management practices and policies should clearly set out governance arrangements for your collection and handling of information using FRT.

These arrangements should ensure you meet your obligations to have an accessible and effective mechanism for receiving and resolving complaints from individuals about your privacy practices. Acting promptly to address complaints can reduce risk, strengthen trust and uncover opportunities to improve your privacy practices.

These practices, policies, and any other relevant governance arrangements should be effectively implemented, documented, and regularly reviewed.

Ensure you keep clear records about how these governance arrangements have been applied in practice.

See Part A of the guidance.

Additional resources

APP Guidelines Chapter 1: Open and transparent management of personal information

OAIC Checklist for privacy dispute resolution (Privacy Awareness Week 2026)