Australian Government

Office of the Australian Information Commissioner

Privacy guidance on age assurance technologies

17 March 2026

OAIC

Contents

Overview 2

Key considerations 2
Who is this guidance for? 3
What is age assurance? 3

Privacy guidance 5

1. Establish whether age assurance is needed (APP 1) 5
2. Uphold anonymity (APP 2) 5
3. Use privacy by design to choose an age assurance method(s) (APP 1) 6
4. Conduct appropriate due diligence (APP 1 & APP 11) 7
5. Build transparency (APP 1 & APP 5) 8
6. Make complaints mechanisms easy to navigate (APP 1) 9
7. Collect minimal data through least intrusive means (APP 3) 10
8. Minimise privacy impacts if using existing information to infer age (APP 6) 13
9. Clearly distinguish a secondary purpose from the primary purpose (APP 6) 15
10. Consider accuracy, bias and discrimination (APP 10) 17
11. Prioritise security and strong vendor controls (APP 11) 18
12. Implement robust de-identification or destruction procedures (APP 11) 19

Overview

Key considerations

- **Establish whether age assurance is needed. Take a privacy by design approach and consider the privacy impacts** associated with each age assurance method (e.g. inference, estimation and verification) and whether the circumstances surrounding the specific chosen method(s) justify the privacy risks. Undertake a Privacy Impact Assessment and implement recommendations to manage, minimise or eliminate privacy risk for each method. (APP 1, APP 2, APP 3, APP 6, APP 10)

- **Undertake due diligence to ensure the security of your entity's age assurance ecosystem** from age check to dispute resolution, especially where multiple providers are involved. Ensure vendors have appropriate governance processes in handling personal information and contractual arrangements ensure privacy compliance. (APP 1, APP 11)

- **When choosing or offering an age assurance method (or combination of methods) ensure it is reasonably necessary and proportionate to legitimate aim(s).** Consider alternate methods and how you can use low-intrusion techniques within an age assurance method(s). Monitor whether the chosen method introduces bias or discrimination. (APP 1, APP 3, APP 6)

- **Escalate to more intrusive personal information handling only as necessary.** Age checks should not seek to reveal the identity of the individual and should only validate age for the purpose of accessing a specific service. Low risk services should consider whether an age check is required or whether self-declaration can be relied upon. (APP 1, APP 3, APP 6)

- **Be transparent, at the moment it matters.** Use APP 5 just-in-time notices to explain key information such as what is collected, why, by whom, how long it is retained, and the individual's choices (including alternative methods and review processes). APP 1 privacy policies should be updated with clear and transparent information, with clear policies and procedures to facilitate this transparency. (APP 1, APP 5)

- **Define primary and secondary purposes precisely** and in line with the specific function or activity for which you are collecting, using or disclosing the information. Descriptions should be clear, concise, up-to-date and visible to individuals when they would reasonably expect it. (APP 1, APP 5, APP 6)

- **Provide clear contact information and ensure meaningful support** is available to individuals, including non-users. Ensure that escalation measures are in place to resolve privacy questions and that complaints processes are simple and accessible in relation to the handling of personal information. (APP 1)

- **Minimise the inclusion of personal and sensitive information in age assurance processes.** Only retain enough personal information in outputs to meet defined purposes, such as to explain the measures implemented for an individual and to facilitate reviews or complaints, then destroy or de-identify on schedule. (APP 3, APP 6)

- **Be thoughtful when designing consent requests** for the collection of sensitive information (such as biometric templates) or for secondary use or disclosure. These should be written and designed so individuals of all abilities can understand what they are being asked to agree to and change their mind. (APP 3, APP 5)

- **Destroy or de-identify any inputs that have been collected immediately once the purposes of collection have been met.** Personal information, including sensitive information, collected for age assurance purposes (e.g. biometric information, biometric templates, identity documents) must be destroyed once all purposes have been met. Avoid purpose 'padding' and ensure destruction includes caches and storage. As a matter of best practice, ringfence inputs by separating out personal information associated with age checks into a contained, secure environment. (APP 11)

Who is this guidance for?

This general guidance is for APP entities considering implementing age assurance systems that collect, use or disclose personal information. The aim of this guidance is to assist APP entities to comply with their privacy obligations under the Australian Privacy Principles (APPs) and support entities and third-party vendors in understanding the privacy impacts associated with choosing and implementing different age assurance systems.

Entities implementing age assurance for the purposes of the Social Media Minimum Age (SMMA) obligation should read this guidance in conjunction with OAIC guidance on Part 4A of the *Online Safety Act 2021* (Cth) which explains the privacy obligations that apply in that context.

What is age assurance?

Age assurance is an umbrella term to describe a range of methods used to verify, estimate or infer an individual's age or age range to determine their eligibility to access, for example, an online service or content. There are multiple broad categories of age assurance, each of which can involve the handling of personal information. Entities may use multiple methods to complete age checks.

Age inference

Age inference commonly uses contextual, behavioural, transactional and/or environmental signals drawn from online activity to imply an individual's likely age or age range. Examples of signals that can be used on their own or in combination to infer age include date of account creation, financial transactions, app settings, linguistic or audio analysis, service usage patterns or participation in age-specific activities.

Signals may be generated through user activity on the service, or may be received from elsewhere, such as an app store, operating system or third-party vendor.

Age estimation

Age estimation uses biometric, artificial intelligence or statistical techniques (such as facial analysis, voice modelling or motion pattern recognition) to examine various data points to predict an individual's age or age range.

Current trends indicate that facial age estimation is the most popular method of age assurance when people are offered a range of options. This solution usually collects a single or burst of selfie photos (plus anti-spoof signals such as liveness detection), either processed on-device or via a third-party provider, to return an age 'yes/no' result.

Age verification

Age verification uses official documents or data sources, such as government-issued IDs, including a driver's licence or passport, to confirm an individual's age. This method verifies age by referencing a verified date of birth and calculating an age from that known data point. Age verification does not usually include identity verification.

Examples include:

- Document check via on-device scan that reads the date of birth (DOB) from a government ID via an on-device app and returns a '16+ yes/no' result.
- Tokenised assertion from a digital identity credential (provided by an accredited identity provider such as a bank, telco or education institution) of the individual's age; no other identity attributes are collected

Self-declaration

Self-declaration is a method where an individual enters or confirms their own date of birth or age or age range.

Parental attestation

Parental attestation (also known as parental consent or vouching) may complement age assurance processes and is a mechanism that enables a parent or guardian to provide or revoke permission for a child.

Privacy guidance

1. Establish whether age assurance is needed (APP 1)

Assessment of risk is a key part of an APP entity's privacy obligations. APP entities should use a risk assessment to help determine if it would be suitable to implement age assurance (including the identification of relevant laws or regulations) and if so, whether the scope of the proposed personal information handling is proportionate to that risk. The OAIC encourages businesses to re-design their services to be safer by default, with age assurance only required for certain higher-risk aspects of the service or compliance with laws or regulations.

Establishing age may not be needed at all if a service, or aspects of a service, can be designed for individuals of any age. APP entities should carefully consider the goals of age assurance, the aspects of their service that are high-risk, and any laws or regulations that require its application.

In some cases, age assurance is required under legislation or regulations (such as under the Social Media Minimum Age obligation and Age-Restricted Material Codes).

Questions to ask

- What risk(s) does the service present to different age groups?
- What is the purpose of using age assurance? Would it mitigate those risks?
- Can you undertake the function or activity without implementing age assurance?
- Is there a clear public interest in using age assurance? Examples may include to comply with a law or regulation.
- Will the use of age assurance lead to unjustified adverse effects, such as unjust discrimination or unjust digital exclusion?

2. Uphold anonymity (APP 2)

Age assurance tools can impact on anonymity or pseudonymity if they are overbroad and unnecessarily document identity rather than an age or age range.

APP 2 provides that an individual must have the option to not identify themselves or use a pseudonym when dealing with an APP entity unless dealing with an identified individual is required or authorised by law, or where it would be impracticable for an APP entity to deal with an unidentified individual.

APP 2 is compatible with age assurance where, for example, an individual can operate anonymously or pseudonymously on a platform after they have been through an age assurance process. Privacy risks arise where age assurance paves the way for a service to collect identity when this is not required.

APP entities should therefore deal with unidentified age assured individuals to the extent practicable unless identity is required or authorised by law.

3. Use privacy by design to choose an age assurance method(s) (APP 1)

Age assurance methods have the potential to interfere with the privacy of individuals to varying degrees. Different scenarios and technologies raise different privacy implications depending on how personal information is handled and the sensitivity of the personal information.

The OAIC encourages entities to adopt a 'privacy by design' approach and undertake a Privacy Impact Assessment (PIA) when selecting an assurance method(s). A PIA is a systematic assessment that identifies the privacy impact on individuals, and sets out recommendations for managing, minimising or eliminating that impact. A PIA demonstrates commitment to, and respect of, individual's privacy.

Entities should consider principles such as necessity and proportionality in implementing chosen technologies and methods, particularly given some age assurance methods may involve the handling of sensitive information (such as biometric templates, behavioural signals) and formal identification documents.

In low-risk settings, an entity may not need to have the highest level of certainty about an individual's age. For example, self-declaration or parental attestation could be a proportionate way of establishing age where a service specifically designed for children seeks to place people into an age band to tailor content relevant to that age cohort. Self-declaration could also be appropriate for low-risk aspects of a service (e.g. signing up for a generic newsletter subscription).

In contrast, lower-confidence methods are unlikely to be appropriate for high-risk settings such as services for general audiences that have interactive features that allow children and adults to co-mingle.

Where more defined age-gates may be required to address higher-risk services or legal requirements, entities may adopt a waterfall approach to age assurance, meaning that more privacy invasive methods are applied only when prior methods are insufficient or inconclusive to validate the age of an individual. Entities may implement multiple methods to achieve this, starting with low-intrusion techniques within an age assurance method(s) and escalating to more intrusive information handling only as necessary.

Entities should also consider the privacy impacts associated with each age assurance method (e.g. inference, estimation and verification) and whether the circumstances surrounding the specific chosen method(s) justify the privacy risks. In determining whether the use of an age assurance method is necessary, entities should consider factors including:

- the suitability and effectiveness in addressing the intended outcome (e.g. preventing access to age-restricted material).
- whether the method is proportionate to the legitimate aim or purpose, particularly where handling of sensitive information is proposed.
- whether the method presents a risk that individuals may be unfairly treated.
- data handling practices associated with the method employed (e.g. security, vendor controls).

- alternative age assurance methods available including whether less privacy-intrusive alternatives are available to address the intended outcome.

It is the responsibility of the entity providing the service to justify that the age assurance method adopted is reasonably necessary. The fact that a particular age assurance method or combination of methods is available, convenient or desirable should not be relied on to establish necessity. Appropriate records recording the reasons for the decision should be kept.

4. Conduct appropriate due diligence (APP 1 & APP 11)

In the current market, various age assurance functions and product offerings are being split across the technology stack. This fragmentation does not absolve an entity from fully understanding the extent to which personal information is handled across the age assurance lifecycle and implementing appropriate governance measures. Due diligence is essential to configuring a solution that is proportionate to the risk of the service and maintaining the integrity of an APP entity's age assurance ecosystem.

It is the responsibility of the organisation seeking to deploy a third-party age assurance solution to ensure it is configured and used in a way that is compliant with the Privacy Act and any other laws or regulations that apply. Before deploying a third-party age assurance solution, organisations should ensure they understand how the product works, identify the potential privacy risks involved and implement measures to mitigate those risks. This is particularly important if the third party is located offshore as you may be held liable for the acts of those third parties.

Prior to entering into a contract with a third party, review the terms of the agreement to understand how personal information is collected, handled and stored, and make sure you are satisfied the third party has appropriate processes in place to protect personal information and comply with any obligations it has under the Privacy Act and any other laws or regulations that may apply. APP entities could consider:

- requesting relevant documentation, such as the third party's privacy policy, information security policy and data breach response plan.
- conduct due diligence, for example by carrying out a quick search for any past security incidents associated with the product or service.
- including contractual arrangements with your service providers to include terms to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled.
- conducting periodic reviews of the personal information handling requirements of the arrangements.
- keep detailed records of your arrangements with the third party to maintain an audit trail and ensure you know what personal information the party holds on your behalf.
- at the end of the contract, ask the third party to confirm that they have deleted any personal information in accordance with the contract terms.

Due diligence for age assurance should not amount to a 'set and forget' approach. To ensure compliance with privacy obligations, organisations should conduct regular reviews of the methods deployed to ensure they are configured appropriately, and that their ongoing use remains reasonable and necessary in the circumstances.

5. Build transparency (APP 1 & APP 5)

The appearance of different age assurance methods and processes can make it difficult for users to understand how their personal information is being handled. Entities should clearly communicate to users through consent requests, privacy policies and notifications why an age check is being conducted and how an age check will take place explaining the specific method(s) and the information handled and any other APP 5 matters.

Any explanations provided should be age-appropriate and specific to the method engaged. Where possible, entities should also present age assurance choices in a way that is equally prominent and offers no detriment for declining one option over another. This is important to ensure that individuals receive the relevant information they need in time to make a meaningful choice.

In higher risk settings where entities need a high degree of certainty, users should also be made aware that they may be subject to multiple methods of age assurance before they are granted access to a service, or specific aspects of a service, or at different times during the course of using the service.

Clear and up-to date privacy policies

Regulated entities are expected to have clearly expressed and up-to-date information contained in their privacy policy about how they collect, use and disclose information in relation to age assurance. As such, updates to privacy policies should be regularly considered to explain the age assurance method(s) in plain English (e.g. inputs, processing, outputs, retention and destruction, vendors, locations, testing / accuracy, and contact points).

Transparency of age inference

Policies should also be clear where entities rely on personal information the entity holds to infer the age of an individual. In this regard, privacy policies should state what signals may be used when age inference processes are completed and provide a high-level overview of how any personal information is handled to generate this output. Examples of signals used for age inference can be seen below.

Examples of signals used for age inference

Age-related signals

- Age of account (e.g. the account has existed for 10 or more years)
- Engagement with content targeted at children or early teens
- Linguistic analysis or language processing
- Analysis of end-user-provided information and posts
- Visual content analysis (e.g. facial age analysis performed on photos and videos uploaded to the platform or entity)
- Audio analysis (e.g. age estimation based on voice)
- Connection with other end-users who appear to be under a certain age
- Membership in youth-focused groups, forums or communities.

Location-related signals:

- IP address, GPS or other location services
- Device identifier, language, time settings
- Phone number
- App store, operating system, account settings

- Photos, tags, connections, engagement, other kinds of activity.

Transparency of third parties

Entities should also provide clear information in their privacy policy regarding any involvement of third-party providers engaged on their behalf to conduct age checks. Entities should provide links to the privacy policies of third-party providers so that individuals can have relevant information up-front and learn more about how entities relate to each other across the age assurance data flow.

Precise and timely notifications

Entities should offer just-in-time notices (APP 5) to individuals at the time of an age check with clear information about their use of specific age assurance method(s).

Notices should include key details about the nature of the age check, including information about:

- Personal information that will be collected during the age check
- The purpose of the age check
- The age assurance method(s) available to the individual (e.g. biometric and non-ID options)
- Third party vendors processing the age check (if relevant)
- The entity or entities who will have access to personal information collected for the age check
- How long inputs / outputs are stored (i.e. retention and destruction processes)
- Appeals and links to additional information about age checks
- Secondary use and disclosure of personal information collected through age checks

6. Make complaints mechanisms easy to navigate (APP 1)

Entities should recognise individuals may be unfamiliar with age assurance methods and could have privacy concerns about the use of the technology as it expands to new contexts.

APP entities must take reasonable steps to ensure that practices, procedures and systems are implemented to deal with privacy enquiries or complaints (APP 1.2).

Entities can demonstrate this by providing simple avenues for individuals to seek information and implementing mechanisms for dealing with enquiries or complaints when things go wrong. Entities may consider developing frequently asked question (FAQ) resources or additional explainer documents to assist with enquiries.

APP entities must also include information within an APP privacy policy about how an individual may complain about a breach of the APPs, and how the entity will deal with such a complaint (APP 1.4). In practice, this means including clear contact information (such as an email address, phone number, mail address, etc.) to enable an individual to easily communicate with an entity about the handling of their personal information. Contact channels should be available to non-account holders and those accessing the service in a logged-out state (including current or former account holders).

Complaint handling processes that are unreasonably complex or overly burdensome for an individual to navigate will not be sufficient to meet compliance obligations under APP 1.

Complaint handling processes and the OAIC

If an individual reports a potential privacy complaint to the OAIC, they will generally be advised that they need to first contact the relevant entity and/or age assurance provider regarding the privacy complaint before it can be lodged with the OAIC. The OAIC will direct individuals to refer to the contact details in the relevant entity/age assurance provider's privacy policy to complain in the first instance.

The OAIC has published resources about the process of lodging privacy complaints on our website.

Practical considerations – transparency and complaints mechanisms

When updating existing privacy policies and procedures to account for information handling associated with age assurance methods, entities may consider developing:

- Standard Operating Procedures for dealing with age assurance enquiries and issues
- Training for relevant internal teams
- A specific age assurance privacy policy
- A Privacy Impact Assessment (PIA) on age assurance methods adopted
- New or updated just-in-time APP 5 notices
- Age-appropriate design and simple language to aid in transparency for likely audiences
- Implementing an accessible log to allow users to see what age assurance method was used, when, if it was shared and with whom

7. Collect minimal data through least intrusive means (APP 3)

Under APP 3.2 and APP 3.3, the collection of personal or sensitive information must be 'reasonably necessary' and must be directly related to one or more of an entity's functions or activities.

When conducting age assurance activities, an APP entity may collect and handle personal information relating to current and prospective users where permitted under the Privacy Act. Age assurance is not a blank cheque to collect and use personal information in all circumstances and should only be used to establish age, not verify an individual's identity. An APP entity 'collects' personal information even if it only holds the information momentarily (e.g. for milliseconds).

Examples of personal information collected for age assurance purposes may include:

- **Inputs** (e.g. document images/text, selfies, biometric templates) that are used for a point-in-time age check.
- **Age artefact** (e.g. 16+ flag) that is created from inputs, existing DOB information on file or inferred from multiple data points.
- **Third-party assertion/token** received from a third-party provider.
- **Documents received** (e.g. Government ID) as part of a formal review or complaint escalation process.

Biometric information and biometric templates

Under the Privacy Act, biometric information that is to be used for the purpose of automated biometric verification or identification (biometric information), and biometric templates (for example those created through the process of facial age estimation) are considered sensitive information. Sensitive information generally has a higher level of privacy protection than other personal information under the APPs.

While an image of a person's face is not considered to be 'biometric information' in every case, it clearly is in some contexts where a biological marker (e.g. fingerprints, the iris or face) is used to produce a unique mathematical representation of those features by the application of technology that applies a mathematical or statistical analysis. In the context of age assurance, the mathematical representation is considered a biometric template and therefore sensitive information. These characteristics are persistent, cannot normally be changed, and are unique to an individual.

APP entities must implement additional safeguards when handling biometric templates and biometric information given the adverse consequences that may arise from the inappropriate handling of such information. Given the sensitivity of biometric templates and biometric information, entities should consider if additional technical or organisational measures are needed to ensure destruction or de-identification has occurred as per APP 11 requirements.

Personal and sensitive information must be collected only by lawful and fair means (APP 3.5). Whether a collection uses unfair means will depend on the circumstances. The collection of personal information to ascertain age should not intimidate or deceive the individual, and any methods engaged should not be unreasonably intrusive to the individual. Entities should also ensure that they do not misrepresent the purpose or effect of the collection, or the consequences for the individual of not providing the requested information to validate their age.

APP entities should consider whether the collection of personal information is reasonably necessary for age assurance purposes. This means considering proportionality, taking a data minimisation approach and choosing the least intrusive way to achieve a clearly defined age result/outcome.

Data minimising age assurance may be as simple as collecting a 'yes/no' result to establish an individual's eligibility to access a service or service feature. An age check is not a vehicle to unnecessarily collect and/or retain identity information about individuals.

Frequency of age checks

Ongoing monitoring (e.g. recurring checks or triggers) should be proportionate and necessary. Any reuse that relies on existing personal information should have consent or another clear legal basis (APP 6). Entities should build and maintain their age assurance practices so that quality (APP 10), security and retention limitations (APP 11) are enforced by design.

Age assurance that is authorised or required by law

APP 3.4(a) (the collection is required or authorised by law) operates in the context of age assurance requirements of specific legal requirements (such as the SMMA obligation) to permit information handling that is necessary in the circumstances to achieve stated legal objectives.

Handling of this information will additionally need to be proportionate to the stated legal objectives to satisfy this necessity requirement.

Where the exception detailed in APP 3.4(a) is not engaged, requirements in APP 3.2 and APP 3.3 apply regardless.

New collections of personal information for age assurance purposes

Where an entity asks an individual to provide certain personal information or go through a process that allows the entity to collect personal information to determine whether the person is 'age-restricted' for the purpose of accessing a service or certain aspects of a service, different methods should be offered to the individual.

Under APP 5, collections of information must be accompanied by clear, age-appropriate notices detailing what personal information may be collected about an individual and the purpose of collection. APP entities should also include the retention period for the personal information.

Practical considerations - collection

The OAIC provides the following practical considerations in relation to collection:

- **Define the outcome precisely** – consider whether a binary age threshold yes/no or age band, (and/or Australian location if necessary) is sufficient. Be clear if the business need requires more than a binary assertion.
- **Test necessity**– Consider whether you can offer processing of personal information at the device level or third-party token instead of methods that involve storing identity documents, biometric templates or biometric information.
- **Prefer less intrusive methods** – where multiple methods can achieve the desired outcome, pick the ones that collect or use less personal or sensitive personal information, require fewer outputs to be stored, and are capable of being destroyed faster.
- **Apply cumulative confidence** – if using existing information to infer age, combine multiple low-intrusion signals that increase the confidence and consistency of the inferred age result/output. Where possible, avoid using behavioural or content data.
- **Minimise what you collect** – where possible, entities should collect binary outcomes ('16+ yes/no') rather than DOB or exact age. In circumstances where a document scan is required, only parse the DOB and redact or avoid non-DOB fields.
- **Process information temporarily** – use technology solutions and/or third-party age assurance providers that temporarily process personal information inputs (e.g., document images/fields, face frames, liveness videos) as part of age assurance and do not retain them. Transient processing of personal information is considered a 'collection' where the information is included in a record.

Case study – minimal collection of personal information

Billie (28) is looking to sign up to an age-restricted service called Manuscript. When completing an age check with Manuscript, Billie chooses an option to verify her age with an age assurance provider called sayID.

sayID is an age assurance provider that orchestrates age checks to be completed through tokens sent from an individual's bank or telco provider.

When Billie selects sayID, she is provided with a clear notice with details relevant to APP 5 including information about the purpose of the age check and third-party vendors involved. The notice also states:

'Manuscript requests that you provide verification of your 18+ status. Do you wish to proceed?'

Billie consents to this notice and is redirected to her banking app where she authenticates sharing an 18+ age token.

In the background, sayID's system sends a request to Billie's bank to send the 18+ age token to Manuscript. No personal information or any banking information is handled by sayID in this process.

Manuscript accepts the 18+ verification and Billie begins to use her new account.

As sayID is acting as an 'orchestrator' to facilitate the age assurance process, there has been no collection of personal information and the entity is not subject to APP 3 requirements in relation to this specific age assurance data flow.

8. Minimise privacy impacts if using existing information to infer age (APP 6)

An entity may choose to use information it already holds about an account holder to infer their age and in certain applications determine whether they are in Australia. This could involve inferring age (or country location) based on behavioural patterns, contextual data, digital interactions, metadata or other information and subsequent collection of an age decision artefact.

Although the use of information for age inference may result in a more frictionless experience for the individual, it may also result in the collection and retention of disproportionate amounts of personal information in a way that undermines individuals' privacy.

Entities must have an appropriate APP 6 pathway in place for conducting age inference using existing personal information:

APP 6.1(a) – Obtain consent from the individual,

APP 6.2(a) – Reasonable expectation and relatedness to the original purpose, and/or

APP 6.2(b) – Required or authorised by law (i.e. s 63D of the *Online Safety Act 2021*).

The application of these pathways is more nuanced in the case of inference due to the wide categories and sensitivities of information that could potentially be reused for inference.

Where an APP entity subsequently creates personal information with reference to, or generated, inferred or observed from, other information the entity holds, this is a 'collection' of personal information and APP 3 obligations will apply.

The OAIC recommends taking a risk-based approach which ensures information used for inference is proportionate and privacy impacts are minimised. This means low volume, less sensitive information should be used over more sensitive information to establish age. It also means that where privacy risks are higher, entities should explore other methods to establish age.

Entities should start with non-sensitive information, low-volume signals; treat outputs as short-lived and ring-fenced; require consent or clear legal basis for any higher-intrusion reuse, especially before taking adverse action. Practices to avoid include always-on monitoring and reusing sensitive information without assessing necessity and proportionality.

Given the breadth of potential information that may be reused for inference, APP 10 (Quality) is especially important. Entities must take reasonable steps to ensure that the personal information involved is accurate, up-to-date, complete and relevant to age assurance purposes.

Entities using age inference should consider:

- whether it has confidence in existing age signals without the need to use behavioural or content data.
- what necessity and consent basis supports this usage where content signals are employed.
- whether the use of existing user signals is reasonably expected (APP 6.2(a)) or whether consent or legal authority is required for entities for age assurance purposes.
- whether a PIA has been conducted and factors demonstrating proportionality have been documented, such as:
    - Sensitivity - how sensitive is the personal information you plan to reuse, and what harm could result if it is wrong or mishandled
    - Volume – how much, how often and for how long will you use personal information for inference and whether adding more signals will materially improve confidence
    - Purpose – whether the reuse is strictly necessary to establish age and nothing more?
    - Relatedness – how closely is the reuse of personal information for age inference related to the original purpose of collection?

9. Clearly distinguish a secondary purpose from the primary purpose (APP 6)

Under APP 6, an APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.

Exceptions include using or disclosing personal information where:

- APP 6.1(a) – Consent is obtained from the individual;
- APP 6.2(a) – Reasonably expected and related to the primary purpose of collection;
- APP 6.2(b) – Required or authorised by law;
- APP 6.2(c) – Permitted general situation exists;
- APP 6.2(d) – Permitted health situation exists; and/or
- APP 6.2(e) – Enforcement related activities (e.g. police investigations).

Entities may have stricter requirements in other regulatory regimes. For example, entities subject to the SMMA obligation should be aware that they must have consent for any secondary use of personal information collected for SMMA compliance purposes must be voluntary, informed, current, specific and unambiguous (refer to the OAIC's guidance on Part 4A of the *Online Safety Act 2021* on this topic).

The OAIC recommends that consent should be the preferred mechanism for the secondary use and disclosure of personal information, unless the circumstances indicate that consent is not appropriate. Consent ensures that individuals are provided with a clear request stating how their information will be used for the secondary purpose and given the opportunity to accept or deny the request.

Entities should not generally rely on a reasonable expectation as the basis for the secondary use and disclosure of personal information collected for age assurance purposes without first assessing whether it is practicable to obtain consent from the individual. As age assurance is a relatively new and emerging technology it may be unfamiliar to most people. This should be factored in when determining whether an individual would reasonably expect their information to be used for secondary purposes.

Regardless of the APP 6 pathway chosen, APP entities should always provide only the minimum amount of personal information necessary to fulfill a secondary purpose.

Use of age artefacts obtained through age assurance methods which are intended for the secondary purpose of direct marketing must also be compliant with APP 7.

Practical considerations – secondary purposes

The OAIC provides the following best practice considerations in relation to secondary use and disclosure:

- **Write a tight purpose statement** – Craft a clear primary purpose statement to be included in the privacy notice / policy. Be clear about related secondary purposes such as compliance and audit. Avoid 'padding' the age assurance purpose with additional purposes such as 'research', 'product improvement' or 'marketing'.

- **Ring-fence outputs** - Segregate age-assurance output data (e.g. binary outcome, method, vendor ID, timestamp and non-linkable token) from other business data stores, so that it cannot be easily co-mingled or used for other purposes.
- **Minimise user outputs** – Provided that transparency and secondary use obligations are met, using existing information directly to confirm whether the individual is over a certain age is a data minimising option because it does not require a new collection or the handling of additional personal information.
- **Document the APP 6 basis** – Assess and record which APP 6 basis applies to the reuse of the information collected.
- **Limit use and disclosure** – use or disclose only binary assertion (e.g. 18+ flag), one-time or short-lived tokens where possible, that are specific as to purpose.
- **Design for users of all abilities** - Present icons, visuals and choices in the user interface. Offer additional clarifying information and prompts to aid comprehension. Implement easy withdrawal toggles in a dedicated privacy setting or contextually appropriate screen.

Case study – secondary use and disclosure with consent

Semicircle is a relevant electronic service that has AI companion chatbot features. It complies with the Relevant Electronic Services Code and conducts age checks via a third party and retains an age artefact indicating the 18+ status of its users and method used.

Alex signs up to Semicircle and undertakes facial age estimation to assure his age.

Later, Alex wants to access another age-restricted service, Triangulation, which also requires users to be over 18 and is linked to Semicircle. On a hand-off screen, Semicircle shows a clear and descriptive just-in-time notice seeking consent:

- Share your 18+ confirmation with Triangulation?
- We can send a one-time '18+ yes' token to Triangulation
- Triangulation will collect and use this token to create your account.
- No name, DOB or other personal information is shared.
- The token will be deleted in 7 days or when you withdraw. Consent can be withdrawn at any time through Semicircle's settings page.
- [Share] [No, I do not wish to share] [Learn more] [Privacy policy]

Alex actively selects [Share]. Semicircle seeks Alex's confirmation for sharing with Triangulation. Upon Alex's confirmation, Semicircle generates a scoped token that encodes only '18+ yes', the method, vendor ID, a timestamp and the duration of consent. It is kept in a separate 'consented-tokens' store, and sent via a secure API to Triangulation.

Triangulation is contract-bound to use the token once, not retain it beyond 7 days, and not disclose to other parties or for other purposes.

Alex is sent a notification that the disclosure was successful and clear, plain-language information about how to easily withdraw consent. If Alex later withdraws consent for sharing, Semicircle sends a webhook to Triangulation and the token is immediately purged on both sides.

Key questions to ask – secondary purposes:

- Is there a specific, narrow purpose for age assurance?
- Which directly related secondary purposes are justified, and which ones are out of bounds?
- Are user-directed secondary uses or disclosures conducted by seeking specific and unambiguous consent, with easy withdrawal?
- Is age-assurance data functionally segregated from other business data stores?
- Do contracts with age assurance vendors mirror our purpose limitations?

10. Consider accuracy, bias and discrimination (APP 10)

Under APP 10, APP entities must take reasonable steps to ensure that personal information collected is accurate, up-to-date and complete. In the context of age assurance, entities should consider the accuracy and effectiveness of the age assurance method(s) being used to perform an age check and ensure that this is proportionate to the potential harm(s) or impact associated with an individual accessing the age-gated aspects of a service. The methods should not create unjustified adverse outcomes to, such as unjust discrimination or unjust digital exclusion.

Given that age assurance methods may sometimes render inaccurate outcomes (specifically due to the estimation of an individual's age), entities should ensure that they have appropriate mechanisms in place for people to appeal an age check. Such processes may assist entities in reducing the number of potential complaints that may be received via other complaints mechanisms (including privacy complaints received under APP 1).

11. Prioritise security and strong vendor controls (APP 11)

Entities must take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure in accordance with APP 11. In age assurance, security is tightly coupled with limited retention and destruction.

Personal information should be processed transiently and not retained, with only a minimal decision record being stored temporarily for declared secondary purposes. Good security also means ring-fencing age assurance data and implementing strong vendor controls, to ensure compliance with APP 11 and other applicable legal obligations.

The OAIC recommends that APP entities undertake rigorous due diligence and maintain strong vendor controls to ensure any third parties engaged for age assurance have effective dispute resolution mechanisms and robust security processes in place to handle individuals' personal information.

Entities should evaluate how third-party solutions integrate with their technical and organisational measures to identify and mitigate any gaps that may exist in the age assurance ecosystem from age check through to accuracy reviews, privacy complaints and retention/reuse. Key security considerations could include factors such as whether inputs collected for age checks are processed at the device level or network level.

APP entities should also validate that any age assurance which requires the disclosure of personal information outside of Australia (regardless of whether the age check is completed via an in-house or third party solution) complies with cross-border disclosure requirements under APP 8 and section 16C of the *Privacy Act 1988*.

Practical considerations – security and vendor controls

The OAIC provides the following best practice considerations in relation to security:

- **Secure and transient processing by design** – Collection flows should be designed so that raw inputs are processed transiently and then destroyed, so that it is not possible to be used or compromised later. On-device processing is recommended to maximise security and limit sharing.
- **Ring-fenced architecture** – retain age assurance data securely in a separate store with its own keys, roles and access controls.
- **Retention automation** – Attach specific time-to-live (TTL) to specified data and purposes and schedule deletion jobs so that they occur automatically.
- **Vendor controls** – Ensure that age assurance vendors are contractually bound by appropriate security and retention provisions. Verify security posture through attestations, audits and other kinds of tests, as necessary.
- **General technical and organisational measures** – Implement strong technical and organisational security measures that surround and support the age assurance method. See the OAIC's 'Guide to securing personal information' and 'Chapter 11: APP 11 Security of personal information' for more detailed guidance.

Key questions to ask

- Are age assurance input data (e.g. selfies, documents, templates) processed transiently and never logged or backed up? Are caches wiped?
- Has only a minimal artefact with a short TTL been retained in accordance with defined purposes?
- Are system mechanisms in place to facilitate automated deletion of personal information collected for age assurance purposes?
- Is age assurance data segregated with its own keys, roles and logs?
- Do contracts ban retention of inputs, require timely deletion and provide for assurance? When was the last time vendor practices were verified?

12. Implement robust de-identification or destruction procedures (APP 11)

De-identification

An APP entity may want or need to de-identify personal information associated with age assurance, such as to provide aggregate level reporting or to comply with obligations under APP 11.

De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. This generally involves removing personal identifiers (e.g. an individual's name or address) and removing or altering other information that may allow an individual to be identified (e.g. rare or unique characteristics of the individual).[1]

Entities should consider a range of relevant contextual factors when determining the de-identification techniques they employ.[2] In the context of age assurance, this could include factors such as the proposed use of the de-identified information or whether any other information or data available could be used for re-identification.

De-identification may not altogether remove the risk that an individual can be re-identified. Entities undertaking de-identification of personal information collected for age assurance purposes are strongly encouraged to undertake a PIA to identify and mitigate any potential risks.

Destruction

Destroying inputs collected during age checks is best practice once the information is no longer needed (i.e. once the age of an individual has been established). This is an important step to reduce privacy and security risks associated with handling personal information and supports compliance with APP 11.2 obligations.

[1] Chapter B: Key concepts | OAIC

[2] De-identification and the Privacy Act | OAIC

Entities should create a distinct 'ring-fenced environment' that enables it to be fully aware of the personal information that it handles for age assurance purposes and where it is kept.

Privacy tip
Good practice includes destruction as soon as age has been verified or estimated by the entity, temporary handling of raw inputs, a ring-fenced minimal artefact, read-only APIs, and automated destruction of personal information used for age assurance purposes. Practices to avoid are retention and use of personal information for its own purposes (e.g., quality assurance, training) without consent or exceptional circumstances

Age assurance inputs (generally higher risk) such as document images/text, selfies, liveness videos, other biometric information or templates and any other personal information that is used as input for an age assurance method.

When handling inputs, APP entities should ensure that:

- Inputs are processed for the purpose of age assurance, and are destroyed immediately following completion
- inputs are not stored 'just in case'
- caches and transient storage are also destroyed.

Age assurance outputs (generally lower risk) including binary outcomes (16+ yes/no), methods, provider IDs, timestamps and non-linkable references/tokens; third-party assertions or tokens received from a third-party provider (such as a bank, telco or education institution). However, APP entities should ensure:

- Any outputs are retained strictly for limited purposes – that is, evidence of compliance, troubleshooting, complaint or review handling, dealing with fraud or circumvention, etc.
- limited retention windows are set.
- The physical/logical separation of outputs through the combination of people, technology and processes to ensure that personal information for age assurance is separated from other parts of the entity and only interface with the entity in limited and controlled ways.
- Documented boundaries are in place to aid compliance and demonstrate accountability, the age assurance environment could be documented in a way that shows the inputs, transient processing, outputs, retention points and destruction paths.
- Destruction readiness in the age assurance environment could be configured such that personal information for age assurance purposes is able to be destroyed.

Entities should also be aware that pre-existing information that is used for age inference is covered by APP 11.2.

Case study – destruction

Quadrangle is an online service that has assessed it must implement age assurance for anyone signing up to the 16+ features of their service in Australia.

1. Destruction example – usual path

Minh picks facial age estimation. Quadrangle uses ProviderX, a specialist age-assurance provider, under a contract that: (i) limits processing to 16+ access-restriction purposes only, (ii) forbids retention of raw inputs, (iii) requires destruction once processing has been conducted, and (iv) provides destruction attestations.

Minh completes a quick blink-and-turn selfie. Ten seconds later, Quadrangle receives from ProviderX only a binary '16+ yes' plus a non-linkable transaction ID. ProviderX automatically destroys the selfie frames and liveness clips. Quadrangle does not store anything from the raw capture. ProviderX's destruction attestation for Minh's transaction is recorded.

In the back-end, Quadrangle writes a small decision artefact into its ring-fenced purpose-built store:

- outcome: 16_plus
- method: face_estimation_v5
- provider_id: ProviderX
- checked_at: 2025-09-18T03:21Z
- token_ref: 9f2a… (opaque)

Quadrangle's product teams can't see this table; they call a read-only /is_16_plus API that returns only 'yes/no'. Advertising, analytics and machine learning pipelines are blocked from the purpose-built store.

2. Destruction example – reviews path

Juliana tries to sign up and follows the blink-and-turn prompts. Ten seconds later ProviderX returns 'cannot confirm 16+' result, which is communicated to Juliana. Quadrangle writes a short-lived 'under_16' decision artefact in the store.

A short explainer appears: "This result is an estimate only. If it's wrong, you can choose another way to confirm your age or start a quick review." Juliana taps 'Review this decision'. The review flow is tightly scoped and clearly explained:

- What she uploads – A photo of an ID page showing only DOB (unnecessary fields are masked in-app).
- Where it goes – A view-only reviews bucket that auto-destroys items after 30 days.
- Who can see it – A single human reviewer in a restricted console; downloads are blocked.

The reviewer checks Juliana's DOB, records '16+ confirmed via review' and hits 'Resolve'. At this point:

- The document image is destroyed; no copies or OCR text is kept.
- The original ‘under_16’ artefact is superseded by a new ‘16_plus’ artefact.

Juliana receives a message saying “Thanks – we’ve fixed this. Your age is confirmed as 16+ and you may proceed to creating your account.”