Australian Government

Office of the Australian Information Commissioner

Privacy Guidance on Part 4A (Social Media Minimum Age) of the *Online Safety Act 2021*

9 October 2025

OAIC

Contents

1. Key considerations 2
2. Overview 3
   2.1. What is personal information in the SMMA context? 3
   2.2. Privacy obligations under the SMMA scheme 5
   2.3. About this guidance 7
3. Adopting a privacy by design approach when choosing an age assurance method or combination of methods 8
4. Privacy guidance – collection 10
   4.1. New collection of information for SMMA compliance purposes 10
   4.2. Using existing information directly to confirm the residency and age of an account holder 12
   4.3. Using existing information to infer the residency and age of an account holder 15
5. Privacy guidance – destruction 19
   5.1. General obligation to destroy personal information 19
   5.2. Information destruction when there are multiple purposes 23
   5.3. Information retention in limited circumstances 24
6. Privacy guidance - secondary use or disclosure of personal information collected for SMMA compliance purposes 26
7. Privacy guidance – frequency of checks 28

1. Key considerations

- **Part 4A of the *Online Safety Act 2021* operates alongside the *Privacy Act 1988* and Australian Privacy Principles.** Part 4A introduces additional, more stringent obligations on age-restricted social media platform providers and third-party age assurance providers when handling personal information for social media minimum age (SMMA) compliance purposes.
- **When choosing or offering an age assurance method (or combination of methods) ensure it is necessary for SMMA compliance purposes and proportionate to the legitimate aim of preventing age-restricted users from having accounts**. Consider alternate methods and how you can use low-intrusion techniques within an age assurance method(s). Escalate to more intrusive personal information handling only as necessary.
- **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 (PIA) when choosing an age-assurance method(s)** to identify potential privacy impacts at the outset and implement recommendations to manage, minimise or eliminate them. This will assist to ensure that a privacy by design approach is embedded from the start.
- **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 a user and to facilitate reviews or complaints, then destroy on schedule.
- **Destroy any inputs that have been collected immediately once the purposes of collection have been met**. Personal information, including sensitive information, that is collected for SMMA compliance 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.
- **Existing personal information used for age assurance does not need to be destroyed where the original purposes for its collection are ongoing**. Using personal information that was collected for a non-SMMA purpose (e.g. age inference) for SMMA compliance purposes does not, by itself, put that information within the remit of s 63F of Part 4A. However, entities must comply with Australian Privacy Principle (APP) 6 to establish the basis for this type of secondary use.
- **Be thoughtful when designing consent requests for secondary uses and disclosures of personal information collected for SMMA**. Secondary use and disclosure should be strictly optional and easily withdrawn. The consent request should be written and designed so users of all abilities can understand what they are being asked to agree to and change their mind.
- **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 user'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.

2. Overview

Part 4A of the *Online Safety Act 2021* (Part 4A) requires a provider of an age-restricted social media platform to take 'reasonable steps' to prevent age-restricted users (under 16 years) from having an account with the platform.[1] The onus is on platforms to introduce systems, processes and controls that can be demonstrated to ensure that people under the minimum age cannot create and hold a social media account.

Part 4A does not prescribe what 'reasonable steps' platforms must take. The eSafety Commissioner (eSafety) is responsible for enforcing compliance with this obligation, and has published regulatory guidance on this topic. However, it is expected[2] that at a minimum, the obligation will require platforms to implement some form of age assurance as a means of identifying whether a prospective or existing account holder is an Australian child under the age of 16 years.

Age assurance is an umbrella term for a set of processes and methods used to verify, estimate and/or infer the age or age range of an individual. This enables platform providers and third-party age assurance providers to make age-related eligibility decisions.[3] These providers are collectively described as 'entities' in this guidance.

Part 4A is technology-neutral and does not mandate any single method or combination of methods. Whether an age assurance methodology meets the 'reasonable steps' requirement is to be determined objectively having regard to the suite of methods available, their relative effectiveness, costs associated with their implementation, and data and privacy implications on users, amongst other things.[4] The Office of the Australian Information Commissioner (OAIC) recommends reading this guidance about entities' privacy obligations alongside eSafety's regulatory guidance about the reasonable steps platforms can take to comply with their safety obligations.

Part 4A recognises that entities undertaking age assurance may handle personal information for SMMA compliance purposes.[2] Part 4A operates alongside the *Privacy Act 1988* (Privacy Act) and introduces additional, more stringent obligations when handling personal information to comply with the SMMA requirement.

2.1. What is personal information in the SMMA context?

For SMMA compliance, information involved in age assurance will likely be personal information because it is information or an opinion about an identified individual, or an individual who is reasonably identifiable. This includes situations where the information is inferred, generated or incorrect.

---

[1] To help you assess if a service is an age-restricted social media platform, consult the self-assessment tool developed by eSafety: How to assess if a service is an age-restricted social media platform | eSafety Commissioner.

[2] Explanatory Memorandum, Online Safety Amendment (Social Media Minimum Age) Bill 2024 (Cth).

[3] ISO FDIS 27566-1 – Information security, cybersecurity and privacy protection - Age assurance systems – Age assurance is a set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organisations to make age-related eligibility decisions with varying degrees of certainty.

[4] Explanatory Memorandum, Online Safety Amendment (Social Media Minimum Age) Bill 2024 (Cth).

In practice, the personal information involved in age assurance may be one or more of the following:

- Inputs – personal information about an individual that is collected and processed by an age assurance technology (e.g. photo, voice, document scan).
- Outputs – the SMMA decision artefact created as part of the age assurance process (e.g. '16+ yes/no' token) and linked to an account.
- Existing personal information – information already held about an account holder.

An individual does not need to be named in the specific information for that information to be personal information. An individual can be 'identified' if they are distinguishable from others. For example, even if a name is not present, it may identify an individual, as it will usually be associated with a record of the user or could be linked back to the person it relates to.

Sensitive information is a subset of personal information that is generally afforded a higher level of privacy protection under the Australian Privacy Principles (APPs) than other personal information. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

'Sensitive information' is a subset of personal information[5] and is defined as:

- information or an opinion (that is also personal information) about an individual's:
  - racial or ethnic origin
  - political opinions
  - membership of a political association
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade association
  - membership of a trade union
  - sexual orientation or practices, or
  - criminal record
- health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates (s 6(1)).

Where there is uncertainty, the OAIC encourages entities to err on the side of caution by treating the information as personal or sensitive information and handle it in accordance with Part 4A and the Privacy Act obligations.

[5] For more detail about sensitive information see Paragraph B.141 in Chapter B: Key concepts | OAIC

2.2. Privacy obligations under the SMMA scheme

Part 4A of the *Online Safety Act 2021* operates alongside the *Privacy Act 1988* (Privacy Act) and APPs. Part 4A introduces additional, more stringent obligations on age-restricted social media platform providers and third-party age assurance providers when handling personal information for social media minimum age (SMMA) compliance purposes.

In summary, Part 4A privacy obligations are:

- **Purpose limitation** (s 63F(1)) – An entity that holds personal information about an individual that was collected for the purpose of (or purposes including) the SMMA obligation must not use or disclose the information for any other purpose. The following exceptions apply:
    - In circumstances where APP 6.2(b), (c), (d) or (e) apply; or
    - With the voluntary, informed, current, specific and *unambiguous* consent of the individual (s 63F(2)).
- **Information destruction** (s 63F(3)) – An entity that holds personal information about an individual that was collected for the purpose of (or purposes including) the SMMA obligation must destroy the information after using or disclosing it for the purposes for which it was collected.

Diagram 1 illustrates these obligations and references the sections of this guidance where the relevant issues are discussed.

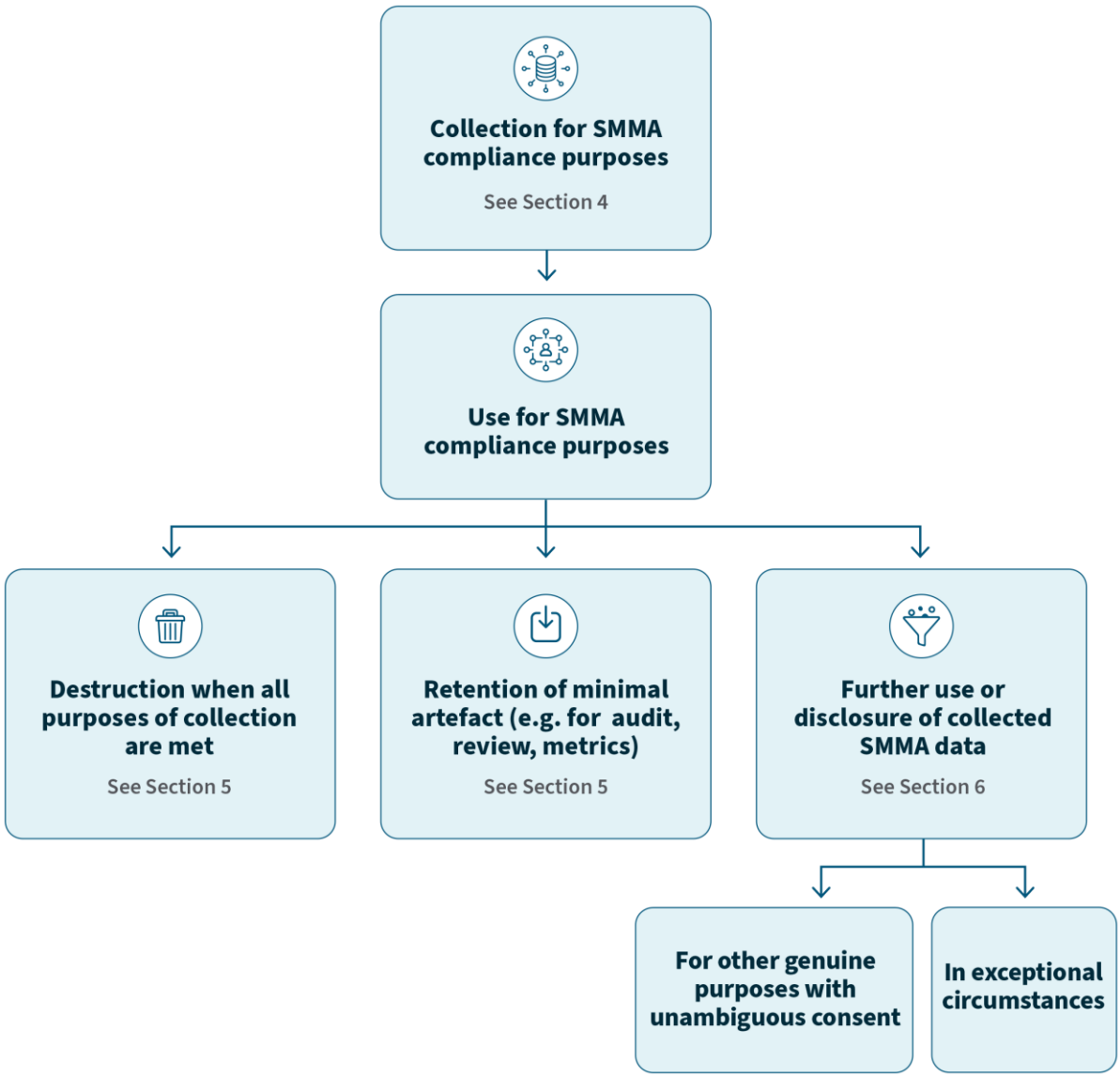

Diagram 1: High-level summary of personal information handling in the SMMA context

Failure to comply with the obligations contained in s 63F is an interference with the privacy of the individual for the purposes of the Privacy Act. This brings non-compliance with s 63F within the remit of the Information Commissioner's enforcement powers under the Privacy Act. It also entitles an individual to complain to the Information Commissioner about an alleged contravention of s 63F.

Steps to comply with the SMMA obligation will not be 'reasonable' unless an entity also complies with its information and privacy obligations under Part 4A, as well as the Privacy Act and the APPs.[6]

[6] See eSafety, 'Social Media Minimum Age Regulatory Guidance' (September 2025) ('eSafety SMMA Guidance').

2.3. About this guidance

Part 4A envisages the processing of personal information for SMMA compliance purposes. The Office of the Australian Information Commissioner (OAIC) has developed this guidance for age-restricted social media platform providers and third-party age assurance providers that must comply with the Privacy Act[7] and Part 4A.[8]

This guidance aims to help entities understand their privacy obligations in the SMMA context. It does not cover the entirety of the privacy obligations that apply and should be read in conjunction with the Privacy Act and the Australian Privacy Principles guidelines (APP guidelines).

Other important resources to review include:

- Guide to developing an APP privacy policy
- Guide to securing personal information
- Guide to undertaking privacy impact assessments

This guidance should also be read in conjunction with eSafety's regulatory guidance on reasonable steps for more information on how to select, deploy and evaluate appropriate age assurance methods and complementary systems and processes for SMMA compliance purposes.[9] eSafety is responsible for formulating the written guidelines for the taking of reasonable steps in relation to the SMMA obligation to prevent age-restricted users from having accounts and associated monitoring, compliance, and enforcement functions associated under Part 4A.

[7] Note that while small businesses with an annual turnover of $3 million or less are generally exempt from the Privacy Act, section 6D(4)(c) of the Privacy Act states that an entity is not considered a small business operator if it discloses personal information about an individual to anyone else for a benefit, service, or advantage. As a result, such an entity must comply with the Australian Privacy Principles (APPs) and other relevant provisions.

[8] Section 63F in Part 4A refers to 'entity', which has the same meaning as in the Privacy Act. Section 63F therefore applies not only to providers of age-restricted social media platforms but also any other entity that handles personal information for the purpose (or one of the purposes) of the SMMA obligation. This includes small business operators.

[9] See eSafety SMMA Guidance.

3. Adopting a privacy by design approach when choosing an age assurance method or combination of methods

Age assurance methods have the potential to interfere with the privacy of individuals. Each scenario, or combination of scenarios, employs different technologies and processes and raises 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 when selecting an assurance method. A Privacy Impact Assessment (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.

This guidance highlights some key privacy considerations for entities to consider, in accordance with the SMMA information lifecycle, particularly regarding collection, use, disclosure and destruction.

Other examples of privacy risks that could be captured and addressed through a PIA include:

- Transparency - the complexity of age assurance methods can make it difficult to understand how personal information is used and how decisions about whether a user is an age-restricted user are reached. Entities should ensure they update their privacy policies (APP 1) and use notifications (APP 5) with clear and transparent information about their use of age assurance methods.
- Accuracy and quality - issues in relation to accuracy or quality of information, particularly for inferred information (see 4.1, 4.3 and 7 below). Entities must comply with their obligation to take reasonable steps to ensure the accuracy of personal information under APP 10 when using age assurance methods.
- Security and data breach - age assurance may increase the risks related to data breaches. This could be through unauthorised access or through attacks. It is important to consider an entity's security obligations under APP 11 and the Part 4A destruction obligations when selecting an age assurance method.[10]

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

Entities should consider low-intrusion techniques within an age assurance method(s) and escalate to more intrusive information handling only as necessary. Entities should also consider the privacy

[10] The concepts of transparency, accuracy and security are also built into the guiding principles eSafety's regulatory guidance puts forward to inform providers' reasonable steps to comply with Part 4A.

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 an age assurance method is necessary, entities should consider factors including:

- the suitability and effectiveness in addressing the SMMA obligation
- whether the method is proportionate to the legitimate aim of preventing age-restricted users from having accounts, particularly where handling of sensitive information is proposed[11]
- alternative age assurance methods available to address the SMMA obligation.

It is the responsibility of the entity to justify that the age assurance method 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.

[11] Sensitive information under the Privacy Act is afforded a higher level of privacy protection and must generally be collected with the individual's consent.

4. Privacy guidance – collection

4.1. New collection of information for SMMA compliance purposes

What it looks like

An entity asks a user to provide certain personal information or go through a process that allows the entity to collect personal information to determine whether the user is an age-restricted user (under 16 years) for SMMA compliance purposes.

Example - Age estimation

- Facial age estimation that collects a single or burst of selfie photos, plus anti-spoof signals; this is processed on-device or via a third-party provider and returns a '16+ yes/no' result.

Example - Age verification

- 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.[12]
- Tokenised assertion from a digital identity credential (provided by an accredited identity provider such as a bank, telco or education institution) that the user is 16+; no other identity attributes are collected.[13]

Privacy considerations

Legal application

Both the Privacy Act and Part 4A apply. In addition to the APPs, entities must comply with the stricter obligations introduced by Part 4A.

APP 3.4(a) (the collection is required or authorised by law) operates in this context to permit information handling that is necessary in the circumstances to achieve the objective of preventing age-restricted users having accounts. Handling will additionally need to be proportionate to satisfy this necessity requirement.

Where the APP 3.4(a) exception is not engaged, the requirement in APP 3.2 and APP 3.3 for collection of personal or sensitive information to be 'reasonably necessary' will apply to

[12] There must be alternatives to this method since this involves government-issued identification – see Online Safety Act, s 63DB.

[13] There must be alternatives to this method if using an accredited service within the meaning of the *Digital ID Act 2024* – see Online Safety Act, s 63DB.

collection of any such information. This limits what information may be collected to those steps that would fulfil a platform's function to comply with s 63D of Part 4A.

APP 5 (Notification of the collection of personal information) and APP 10 (Quality of personal information) are also of particular relevance when collecting personal information for age assurance.

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

Minimise what you collect

- Where possible, collect binary outcomes ('16+ yes/no') rather than DOB or exact age.
- If scanning a document, 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.

Good practice case study – collection of information for age check at sign-up

GlowLoop is a social media app that must comply with the SMMA obligation. At signup, any prospective user in Australia (determined by a one-off country signal using IP address[14]) sees a short explainer screen:

"Before we create your account, we need to confirm you're 16 or over. Pick the option that suits you. We don't keep your photos or documents." [How we handle your personal information]

Tapping the 'How we handle your personal information' opens a simple APP-5 compliant notice dialogue box.

Users can choose between two big tiles, side-by-side:

1. Digital ID (myID) / device-wallet token

"Use a credential to share a simple 16+ yes/no with GlowLoop. No other details collected."

[14] eSafety's SMMA Guidance also notes where providers seek to rely on IP addresses to identify whether a user is ordinarily a resident in Australia, they should also take steps to detect the use of VPNs and consider additional signals that may indicate a user is in Australia (p 33).

2. Facial age estimation (no selfie storage)

"Take a quick selfie on this device. We'll process it to estimate if you're 16+. We don't save the images."

Eva (20) chooses facial age estimation. The app asks her to hold the phone steady and blink; a short progress ring spins. Ten seconds later, she sees: "You appear to be 16+. Continue to create your account." The app explains that Eva's selfie was processed locally and not stored. She taps Continue and finishes signing up.

Sam (24) chooses Digital ID. His phone opens a device wallet card issued by his bank (which supports age assertions); he consents to sharing a "16+" assertion only. Back in GlowLoop, he sees: "We received a 16+ confirmation. You're set." The app explains that no document numbers or dates of birth are shared. Sam taps Continue and finishes signing up.

Kendra (17) tries facial age estimation first. The result comes back borderline, so GlowLoop returns Kendra to the previous page to choose again between facial age estimation and government-issued ID. Kendra selects the drivers licence-issued digital credential in her wallet, shares a binary 16+ assertion, and completes sign-up.

Privacy tip:

Good practice includes instant destruction of raw selfies; short-lived, scoped tokens; and ring-fencing the minimal decision artefact (e.g. binary outcome, method, provider ID, timestamp, non-linkable token). Higher risk practices include storing selfie frames, logging tokens in a way that enables cross-service tracking, or making the escalation automatic without clear consent and alternatives (e.g. forcing a government-issued ID or accredited Digital ID upload).

4.2. Using existing information directly to confirm the residency and age of an account holder

What it looks like

An entity uses information it already holds about a user to directly determine whether they are under 16 years. This is typically done to detect and deactivate accounts belonging to age-restricted users. Using existing information to *infer* the age or location of a user is discussed separately in Section 4.3.

- Example - Existing DOB or self-declared age on file is referenced.
- Example - Existing third-party assertion or token (e.g., from a telco, bank or digital wallet) confirming 16+ is still within validity.

Privacy considerations

Legal application

Part 4A

The s 63F obligations in Part 4A apply to personal information that was collected for SMMA compliance purposes. If an entity uses information it already holds to conduct age assurance and no new collection occurs, then s 63F will not apply. Using personal information that was previously collected for a different purpose does not, by itself, put that information within the remit of s 63F.

However, if the entity creates a new piece of information for SMMA compliance purposes (e.g., using the existing DOB on file to create a new '16+ flag' for the account holder), that new artefact would constitute a collection that is subject to s 63F.

Privacy Act

The APPs continue to apply in this scenario, including where information is generated or inferred.

It will be particularly important for the entity to comply with APP 6 (Use and disclosure) and identify and document an appropriate pathway for the secondary use of 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 Part 4A).

Diagram 2 below explains the process for determining the most appropriate pathway.

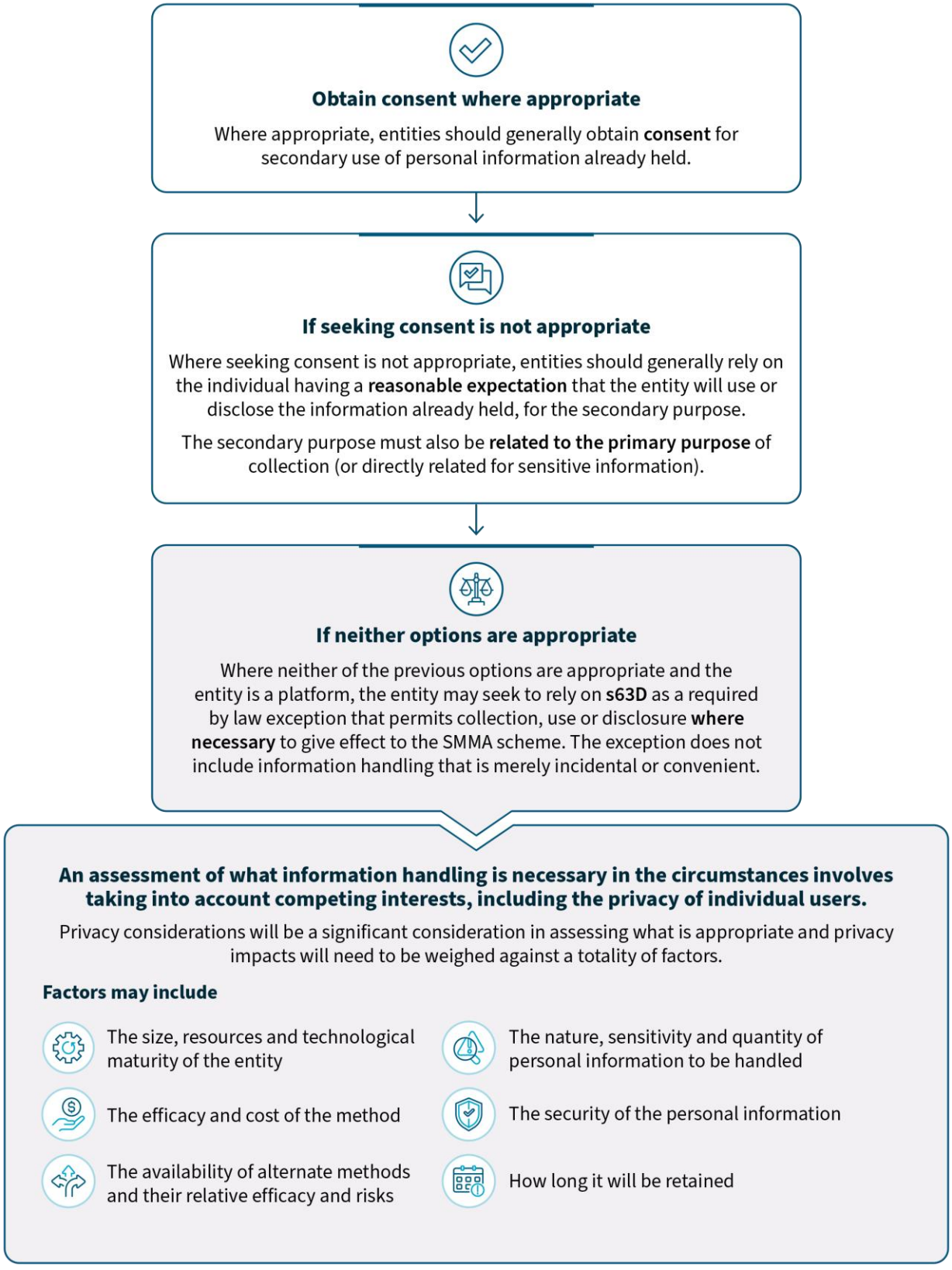

Diagram 2: APP 6 considerations when seeking to use personal or sensitive information for SMMA compliance purposes

Practical Considerations

The OAIC provides the following practical considerations when using existing information directly to comply with the SMMA obligation:

Minimise what you use

- As long as the transparency and secondary use obligations are met, using existing information directly to confirm residency and whether the user is over 16 is a data minimising option because it does not require a new collection or the handling of additional personal information.
- Use only the fields that are needed to determine age or residency.

Document the APP 6 basis

- Assess and be able to demonstrate the APP 6 basis for information reuse.

Handle sensitive information carefully

- Be very cautious if using existing biometric templates, images or other sensitive kinds of information for SMMA compliance purposes.
- Ensure handling is necessary and proportionate to comply with the requirements of s 63D. If unsure, establish a clear expectation from the user and ensure a close relationship to the primary purpose of collection; otherwise obtain consent.

4.3. Using existing information to infer the residency and age of an account holder

What it looks like

The entity uses information it already has about the account holder to infer whether they are under 16 years and whether they are ordinarily resident in Australia. This could involve drawing probabilistic conclusions based on behavioural patterns, contextual data, digital interactions, metadata or other information and subsequent collection of a 16+ decision artefact.

Examples include:[15]

Location-related signals

- IP address, GPS or other location services
- Device identifier, language, time settings
- Phone number

[15] Extract from eSafety's SMMA Guidance, p 32.

- App store, operating system, account settings
- Photos, tags, connections, engagement, other kinds of activity.

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 16
- Membership in youth-focused groups, forums or communities.

Privacy considerations

Legal application

Part 4A

Inference would be typically conducted using information that was not collected for SMMA but rather other purposes, such as account management, safety and content moderation, providing core features and services, etc. Therefore, s 63F will not apply to the original inputs.

Where an entity uses inference methods to generate personal information (e.g. +/-16 score, pass/fail age flag, Australian resident flag), the resulting new artefact will be considered a collection of personal information and is subject to the restrictions in s 63F including purpose limitation and destruction (see Section 5 of this guidance).

Privacy Act

The APPs continue to apply in this scenario, including where information is generated or inferred.

It will also be important for the entity to have an appropriate APP 6 pathway for conducting inference on 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 Part 4A).

While the APP 6 pathways for use of existing information for inference is the same as use of existing information directly to comply with the SMMA obligation, their application is more nuanced in the case of inference. This is due to the wide categories and sensitivities of information that could potentially be reused for inference.

See Diagram 2 above.

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 the SMMA obligation.

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.

Practical considerations

Different cohorts of users may require different approaches. eSafety guidance confirms there is no one-size-fits-all approach that will be suitable in all circumstances. For a substantial proportion of users on long-standing platforms, it may be possible to confirm at a high level of confidence that they are 16+ years old based on the account tenure or creation date. More work, effort and personal information will be required to infer age where account tenure is short, or where the user is in a younger age threshold.

The OAIC recommends taking a risk-based approach which ensures information used for inference is proportionate and privacy impacts are minimised. This means less sensitive information is preferred over more sensitive information Ito achieve an acceptable inference outcome. It also means that where privacy risks are higher, entities should explore other methods for age assurance.

The OAIC provides the following proportionality considerations tailored to age inference, drawing on the factors outlined in Section 4.2 above:

Sensitivity – How sensitive is the personal information you plan to reuse, and what harm could result if it is wrong or mishandled?

- Prefer non-sensitive information, non-content signals such as metadata and system data.
- Treat behavioural and content data (e.g. posts, events, groups, interests, affinities, communications and other user interactions) as higher privacy risk.

Volume – How much, how often and for how long will you use personal information for inference?

- Use event-based, point-in-time checks.
- Avoid building long-lived behavioural profiles; only add more signals if they materially improve confidence.

Purpose – Is the reuse strictly necessary to achieve the SMMA decision and nothing more?

- Define the outcome precisely and assess whether inference is an effective method.
- Use a less intrusive method if it can deliver the same outcome while using less personal information.

Relatedness – How closely is the reuse of personal information for age inference related to the original purpose?

- Ask whether an individual would reasonably expect the personal information to be reused for age assurance purposes.

eSafety's regulatory guidance provides further detail on assessing the reliability, accuracy, robustness and effectiveness of age inference as a method of age assurance.

To minimise privacy impacts on individuals, the OAIC recommends handling less sensitive information over more sensitive information (e.g. age analysis performed on photos and videos, or audio analysis on voice), to achieve an acceptable inference outcome. It also means that where privacy risks are higher, entities should explore other methods for age assurance.

Good practice case study – inference using existing signals

VibeTrail is a social media platform. Once the SMMA obligation takes effect, VibeTrail implements a back-end system that uses information it already holds to infer (a) whether an account holder is ordinarily resident in Australia and (b) whether they are under 16. It doesn't ask existing account holders for age checks, unless the inference raises a doubt about whether they are over or under 16.

1. 'Long-time user in Australia'

Alan (45) has used VibeTrail for twelve years. His language/time settings are English (AU)/Australia, and he signs in from an AU IP address.

These signals may reflect a proportionate secondary use of personal information to reasonably infer 'resident in Australia' and 'likely 16+'. Alan continues to use his account without experiencing any additional prompts. Use of additional existing information may be considered disproportionate or unreasonable in the circumstances.

2. 'Borderline new account'

Tia (16) created an account one month ago, before the SMMA obligation commenced. Signals show AU IP address and an AU phone number attached to the account but as the account duration is short and there have been no prior age checks, it may be proportionate and reasonable to use other existing personal information to trigger a more reliable age assurance method. For instance, her public bio says 'Year 10 goalie'.

The system flags the account as 'possibly under 16' and shows Tia an in-app notice explaining why. She is offered a choice to resolve it (for example, Digital ID yes/no token, or on-device facial age estimation). If she doesn't act, the account is restricted.

Privacy tip:

Use inference proportionately. 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.

5. Privacy guidance – destruction

5.1. General obligation to destroy personal information

What it looks like

When conducting age assurance activities to comply with the SMMA obligation, an entity will likely collect and handle **personal information** relating to current and prospective users.

Examples include:

- **Inputs (e.g. document images/text, selfies, biometric information, biometric templates)** that are used for a point-in-time age check.
- **SMMA 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 as part of a formal review or complaint escalation process** to comply with the SMMA obligation.

Privacy considerations

Legal application

Section 63F(3) of Part 4A states that an entity that holds personal information about an individual that was collected for the purpose(s) of the SMMA obligation must destroy the information after using or disclosing it for the purposes for which it was collected.

Section 63F(3) is a stricter standard than APP 11.2 (retention of personal information) in two key ways:

1. The information must be destroyed; there is no allowance for de-identification.

2. The destruction must happen once all the purposes for which the personal information was collected during age assurance is met; there is no allowance for retention just because there is another potential business use case.

APP 11.2 continues to apply to all other personal information handled by entities.

Pre-existing information that is used directly to comply with the SMMA obligation or for age inference is covered by APP 11.2 rather than s 63F. However, any new record created from this process for the purpose of the SMMA obligation is covered by s 63F.

You can find more information on security responsibilities in the Guide to Securing Personal Information, and Chapter 11: APP 11 Security of personal information.

Practical considerations

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

Distinguish between inputs and outputs

- Age assurance **inputs** (generally higher risk) – examples include 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.
  - Process for the purpose of age assurance, then destroy immediately
  - Do not store inputs 'just in case'[16]
  - Ensure destruction covers caches and transient storage.
- Age assurance **outputs** (generally lower risk) – examples include 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).
  - Retain strictly for limited purposes – that is, evidence of compliance, troubleshooting, complaint or review handling, dealing with fraud or circumvention
  - Set bright-line, limited retention windows.

Ring-fence the age assurance outputs

- To ensure compliance with the s 63F destruction obligation, the entity should create a distinct ring-fence or 'SMMA environment' that enables it to be fully aware of the outputs that it handles and where they are kept.
- Different entities will have different implementation arrangements. For example:

[16] eSafety's SMMA guidance does not expect providers to retain this information as a record of individual age checks. See eSafety's SMMA guidance on what information may be relevant for compliance purposes.

- **Physical/logical separation** – Combination of people, technology and processes to ensure that personal information for SMMA is separated from other parts of the entity and only interface with the entity in limited and controlled ways.
- **Documented boundary** – To aid compliance and demonstrate accountability, the SMMA environment could be documented in a way that shows the inputs, transient processing, outputs, retention points and destruction paths.
- **Destruction readiness** – The environment could be configured such that personal information for SMMA is able to be destroyed automatically and independently of other organisational data.

There may be legitimate business reasons for co-mingling personal information for SMMA with other personal information (e.g. processing them in shared pipelines or storing them in shared databases). However, this may make it harder to prove purpose limitation and to comply with the strict destruction obligation. Each entity needs to make its own assessment, considering the compliance requirements in s 63F of Part 4A.

The most straightforward path to compliance, and the one that best aligns with the intention of s 63F, is to ring-fence personal information collected for SMMA compliance purposes.

Good practice case study – destruction

GlowLoop is a social media app. After the SMMA obligation takes effect, GlowLoop decides anyone signing up in Australia must pass an age check.

1. Destruction example – usual path

Daniel (25) picks facial age estimation. GlowLoop uses ProviderX, a specialist age-assurance provider, under a contract that: (i) limits processing to SMMA purposes only, (ii) forbids retention of raw inputs, (iii) requires destruction once processing has been conducted, and (iv) provides destruction attestations.

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

In the back-end, GlowLoop writes a small decision artefact into its ring-fenced 'SMMA store':

- outcome: 16_plus
- method: face_estimation_v3
- provider_id: ProviderX
- checked_at: 2025-09-18T03:21Z
- token_ref: 9f2a… (opaque)

GlowLoop'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 SMMA store.

2. Destruction example – reviews path

Aria (16) tries to sign up and follows the blink-and-turn prompts. Ten seconds later ProviderX returns 'cannot confirm 16+' result, which is communicated to Aria. GlowLoop writes a short-lived 'under_16' decision artefact in the SMMA 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." Aria 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 (other 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 Aria'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.
- Aria receives a message saying "Thanks – we've fixed this. Your age is confirmed as 16+ and you may proceed to creating your account."

Privacy tip:

Good practice includes destruction-on-decision by the entity, temporary handling of raw inputs, a ring-fenced minimal artefact, read-only APIs, and automated destruction of personal information used for SMMA compliance 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.

5.2. Information destruction when there are multiple purposes

What it looks like

Section 63F(3) of Part 4A acknowledges there may be multiple purposes for which the personal information is collected, as long as compliance with the SMMA obligation is one of them. A relevant consideration for destruction is what happens in such circumstances, especially where one or more of the other purposes may require the information to be retained for longer than compliance with the SMMA obligation.

Examples include:

- **Sign-up age check –** User completes facial age estimation to open an account. The same event creates a short-lived decision artefact for audit logging and reviews purposes.
- **One age gate, several compliance needs –** A single age check is used to satisfy the entity's obligations with respect to (i) SMMA and (ii) another jurisdiction's age rule.
- **Know Your Customer flow for creator –** An ID and selfie are captured for AML/CTF onboarding; the entity also needs to know that the creator is over 16 years to comply with the SMMA obligation.

Privacy considerations

Legal application

Section 63F(3) of Part 4A requires the entity to destroy the information collected for the SMMA obligation, once it has used or disclosed the information for all the purposes for which it was collected.

Practical considerations

The OAIC provides the following practical considerations when considering destruction in the context of multiple purposes:

Avoid 'purpose padding'

- Consistent with Chapter 6 of the APP Guidelines, purposes must be construed narrowly and not be so general in nature that they comprise a function or activity of an entity. Do not include broad, speculative or open-ended purposes as part of collection for age assurance (e.g. product improvement, research).
- Additional purposes must be genuine. Merely asserting that the collection is for other purposes does not allow you to retain the information collected for longer than compliance with the SMMA obligation.

Develop a retention matrix

- Where the information collected (e.g. SMMA artefact) serves multiple purposes, ensure that each purpose has a defined retention period and destroy the information once the last retention period has expired.

Further partition the personal information where there are additional requirements

- If a different legal regime (e.g. AML/CTF, overseas jurisdiction) requires retention following an age check, produce and retain separate non-SMMA artefacts or records.

5.3. Information retention in limited circumstances

What it looks like

There are narrow situations where an entity may need to retain a minimal record after an age check to operate the service responsibly and evidence compliance.

Examples include:

- Audit logging and evidence of compliance – Prove that a check has occurred, the outcome, how it was done, and when.
- Troubleshooting, fraud and circumvention – Investigate errors, suspected spoofing and re-registration attempts.
- Complaints and reviews – Respond to user/parent challenges to the age check or its outcome.

In such cases, it is sufficient that a SMMA artefact is collected and retained, which contains minimal information such as binary outcome (16+ yes/no), method, provider ID, timestamp and non-linkable reference/token.[17]

Privacy considerations

The OAIC considers that tightly limited retention of personal information is acceptable and can be done in accordance with Part 4A and the Privacy Act.

All the practical considerations above regarding destruction in the context of multiple information collection purposes are applicable here. In particular, the entity should be transparent about the directly related purposes arising from the age check that involve retention for a longer period.

The one additional consideration is for entities to set time-based limits for each purpose that involves personal information for SMMA (e.g. evidence of compliance, troubleshooting, complaints and

[17] This is consistent with eSafety's guidance that platforms are not expected to retain personal information as a record of individual age checks (eSafety SMMA Guidance, p 25). Although note that to the extent SMMA artefacts are linked with users or account information, they may be considered personal information.

reviews). The timing should be justified by the business practice and accord with standard industry practice.

The time-limits for each purpose should determine when and how the personal information is accessed and used. Once the time period for the last allowed purpose has expired, the entity should destroy the relevant artefact.

Privacy tip - example do's and don'ts for good practice

Audit evidence, proof a check occurred

- Do retain a minimal decision artefact (e.g. binary outcome, method, provider ID, timestamp, non-linkable token), with documented retention periods; enable auto-destroy.
- Don't store selfie frames, ID images, biometric templates or age scores/confidences that are no longer required.

Troubleshooting, fraud and circumvention

- Do retain the minimal artefact for a case-linked time window; require a Case ID; purge once case is closed.
- Don't build open-ended watchlists or keep biometric templates or raw documents indefinitely 'in case of future abuse'.

Complaints and reviews

- Do accept redacted DOB evidence in a view-only bucket; destroy the document immediately after the decision; keep only the updated minimal. Don't keep copies of documents or OCR text beyond the review; store full DOB or document numbers in the SMMA store.

6. Privacy guidance - secondary use or disclosure of personal information collected for SMMA compliance purposes

What it looks like

An entity may seek to reuse age assurance inputs for other business purposes or disclose the output (e.g. 16+ artefact) to another entity.

Privacy considerations

Legal application

Section 63F(1) of Part 4A restricts the use or disclosure of personal information collected for the SMMA obligation. Secondary use or disclosure is only permitted with the unambiguous consent of the individual, or in exceptional circumstances outlined below.

The definition of consent in s 63F(2) is notable for including 'unambiguous' as one of the elements of consent. This is a requirement specific to the SMMA scheme that precludes entities from seeking consent through pre-selected settings or opt-outs.

'Exceptional purposes' align with the following paragraphs in APP 6.2 (refer to Chapter 6 of the APP Guidelines for further information on these exceptions):

- Para 6.2(b) – It is required or authorised by or under an Australia law or a court/tribunal order. For example, a subpoena or statutory notice compels the disclosure of the SMMA artefact for specific users.
- Para 6.2 (c) – A permitted general situation exists. For example, use of the SMMA artefact to triage a suspected unlawful security breach as part of a security incident response.
- Para 6.2 (d) – A permitted health situation exists. For example, a credible, serious safety threat necessitates disclosure of the SMMA artefact to an emergency health services provider.
- Para 6.2 (e) – The organisation reasonably believes that it is necessary for one or more enforcement related activities. For example, an enforcement body requests information for enforcement related activities (see Chapter B of the APP Guidelines).

Practical considerations

The OAIC provides the following practical considerations when seeking to use or disclose personal information used for SMMA for secondary purposes with unambiguous consent.

Consented purposes

- **Limit what you use and disclose:** Use or disclose only a binary assertion ('16+ yes'), one-time or short-lived tokens where possible, that are specific as to purpose.
- **Make consent truly optional:** Implement a separate consent flow dedicated to secondary purposes; do not bundle with the SMMA purpose. Avoid general or broad terms of use or agreement obtained through use of dark patterns. Set defaults to 'off'.
- **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.

Exceptional circumstances

- Exceptional circumstances are non-routine. However, as a matter of best practice, it is useful for entities to have processes in place to deal with them. For example:
  - Identify the presenting issue and which APP 6.2 exception is relevant.
  - Apply a necessity and proportionality test to determine whether use or disclosure is warranted.
  - Default to using or disclosing the minimum amount of information required.
  - Keep a record of the decision(s) made and action(s) taken.

Good practice case study – Secondary use and disclosure with consent

FlareHub is a social media platform. It complies with the SMMA obligation and conducts age checks on its users, retaining a SMMA artefact indicating that a user is 16+.

David (22) signs up to FlareHub and undertakes facial age estimation to assure his age.

Later, David wants to join a music community, StageDoor, which also requires users to be over 16 and is linked to FlareHub. On a hand-off screen, FlareHub shows a clear and descriptive just-in-time notice seeking consent:

- Share your 16+ confirmation with StageDoor?
- We can send a one-time '16+ yes' token to StageDoor
- StageDoor 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 FlareHub's settings page.
- [Share] [No, I do not wish to share] [Learn more] [Privacy policy]

David actively selects [Share]. FlareHub seeks David's confirmation for sharing with StageDoor. Upon David's confirmation, FlareHub generates a scoped token that encodes only '16+ yes', the method, vendor ID, a timestamp and the duration of consent. It is kept in a 'consented-tokens' store, separate from the SMMA data store, and sent via a secure API to StageDoor. StageDoor is contract-bound to use the token once, not retain it beyond 7 days, and not disclose to other parties or for other purposes.

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

Privacy tip:

Good practice involves outputs-only sharing via a one-time, partner-scoped token; separate token stores; clear and descriptive just-in-time notices; and a separate, unambiguous opt-in for a clearly described purpose and time period. Do not bundle consent at sign-up or use pre-selected tick boxes.

7. Privacy guidance – frequency of checks

The SMMA guidance issued by eSafety observes that the measures taken by platforms to comply with the SMMA obligation should not be static. Rather, '[p]roviders should proactively monitor and respond to changes in their platforms' features, functions, and end-user practices, especially where these or other changes may introduce new risks.'[18] Furthermore, eSafety expects platforms to take proactive steps to detect accounts held by age-restricted users on an ongoing basis.

The OAIC notes that steps taken by entities to comply with the SMMA obligation on an ongoing basis will likely handle personal information (including collection and reuse) in ways that are addressed by the preceding sections.

Ongoing compliance (e.g. recurring checks or triggers) should be proportionate and necessary to comply with the SMMA obligation. 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.

[18] See eSafety SMMA Guidance, p 29.