dspanz. digital service providers australia new zealand

Privacy and Identity Verification

Best Practice Guidance for Digital Service Providers

Version 1.0
18 December 2025

Contents

About DSPANZ

DSPANZ represents the business software industry across Australia and Aotearoa New Zealand. Our members develop software that enables over 90% of payroll, superannuation and tax transactions, supporting employers, employees and trusted advisors with their day-to-day business operations.

Purpose of the Guidance

This best practice guidance has been developed in response to the ongoing risks associated with customers collecting and storing proof-of-identity documents in software, and to highlight the benefits of using identity verification software solutions, whether used directly or through integration with third-party providers.

While this document is primarily intended for Digital Service Providers (DSPs) offering tax, accounting, payroll, superannuation, employer obligations, business registry, and invoicing software, other software providers and businesses can also benefit from this best practice guidance.

The outcomes of this guidance are to:

- Eliminate the storage and retention of identity documents and associated data within software by default.
- Enable the development of systems and processes supporting identity verification in software that align with privacy and data protection principles under Australian and New Zealand law.
- Encourage the adoption of digital identity verification solutions.
- Support the creation of educational materials for DSP customers about identity verification best practices.

Scope of the Guidance

This guidance considers how DSPs support customers in meeting their identity verification requirements while using software. DSPs may offer software products and services that handle, transmit, or process personal identity information captured during registration, onboarding, or compliance workflows.

In scope:

- Verification of identity practices.
- Creating audit records to capture when identity verification events occur.
- Destroying identity documents and personal information after verification.

Out of scope:

- Regulatory requirements specifying the types of identity documents or information that must be verified.
- Identity or personal information that may be collected or verified as part of a compliance or business process and is ultimately retained as part of a customer or user record.
- Business or corporation identity verification.

Definitions

Identity information in this guidance document refers to any data extracted from personal identity documents (for example, passports or driver's licences), including images, identification numbers, metadata, or scanned text, used for verification purposes.

Metadata retained for audit purposes (such as system timestamps or reference numbers) is not considered personal information.

Permanent deletion in this guidance document means the complete deletion of all identity documents (including any backups), once verification and any risk activities are complete.

Introduction

Digital Service Providers (DSPs) handle sensitive personal information at scale and play a critical role in helping customers meet identity verification and know your customer requirements. As these obligations increase across industries, organisations rely on their software to support compliant and secure verification processes.

Identity verification introduces additional privacy and security risks, particularly when identity documents can be uploaded or stored within software products. Unnecessary storage of identity documents heightens the impact of data breaches and the risk of regulatory action.

While current practices rely heavily on physical identity documents and manual processes, emerging digital identity solutions and verifiable credentials will continue to reshape how DSPs support identity verification.

This *Privacy and Identity Verification: Best Practice Guidance for DSPs* outlines how software providers can implement privacy-centric, digital-first verification processes that protect end users, meet legislative obligations, and minimise data retention. The guidance focuses on enabling customers to record that verification events have occurred without storing identity documents.

The document supplements identity verification requirements in Australia and Aotearoa New Zealand and provides practical recommendations for software design and implementation. It explains how DSPs can meet the best practice principles, including:

1. Enable digital-first identity verification
2. Prevent the upload or storage of identity documents
3. Delete identity documents after verification
4. Retain metadata only
5. Protect verification data (security, audit, and assurance)
6. Be transparent with users.

The best practice guidance is also designed to follow the Australian *Privacy Act 1988*, the Australian Privacy Principles (APPs), the New Zealand *Privacy Act 2020* and the New Zealand Information Privacy Principles (IPPs).

The DSPANZ Digital Identity Working Group has developed this guidance in collaboration with industry and government partners. It is a living document and will be updated as technologies and regulatory frameworks evolve.

Further guidance on digital identity, data minimisation and secure information handling is available on the DSPANZ website.

Best Practice Principles

Principle 1: Enable digital-first identity verification

DSPs should offer digital identity verification processes to customers by default.

Digital identity verification methods reduce the need to handle physical documents, improving privacy and security.

DSPANZ strongly recommends that DSP software products should not store or retain copies of identity documents beyond the immediate purpose of verification.

Best Practice Guidance

1.1. Adopt digital identity verification methods by default. Identity verification processes should provide an audit record with metadata that retains verification outcomes.

1.2. If digital identity verification can not be used, DSPs may support in-person verification without allowing customers to store copies of identity documents and enabling the recording of metadata for audit purposes.

This principle relates to the following Australian (APP) and New Zealand (IPP) privacy principles:

- APP 1: Open and transparent management of personal information
- APP 3: Collection of solicited personal information
- IPP 1: Purpose for collection of personal information
- IPP 3: Collection of information from subject - what to tell the individual.

Principle 2: Prevent the upload or storage of identity documents

DSPs should determine whether their software products enable customers to upload or store identity documents (for example, copies of passports or driver's licences) used to support verification processes.

DSPs that provide document upload functionality are at high risk of customers or users leveraging this to store identity documents.

Enabling the upload or storage of identity documents can result in unintentional data retention and the exposure of identity information in the event of a data breach.

Best Practice Guidance

2.1. DSPs that provide document upload functionality should include explicit references in software terms and conditions about customers or users not using this functionality to upload and store identity documents.

2.2. DSPs that enable document upload functionality should consider using technology that can identify identity documents and prevent them (and any personal identity information) from being uploaded.

2.3. Communicate to customers that storing copies of identity documents in software products is considered a breach of terms and conditions and should be identified and removed.

2.4. DSPs that can confirm if identity documents have been stored in software should:

- Contact the customer and inform them that stored identity documents have been identified;
- Provide an opportunity for the customer to record verification outcomes; and then
- Permanently delete any stored documents.

This principle relates to the following Australian (APP) and New Zealand (IPP) privacy principles:

- APP 3: Collection of solicited personal information
- APP 11: Security of personal information
- IPP 1: Purpose of collection of personal information
- IPP 5: Storage and security of information.

Principle 3: Delete identity documents after verification

DSPs and their customers should permanently delete any identity documents used to support identity verification after the verification process is complete. This principle applies to all forms of identity documents, including, but not limited to, passports, driver's licenses, and birth certificates.

DSPs should record only the outcomes of identity verification.

Retaining copies of identity documents increases the risk and severity of a data breach. DSPs covered by privacy legislation across Australia or New Zealand may be required to report eligible data breaches.

Best Practice Guidance

3.1. Identity documents should be automatically and permanently deleted once the verification of an individual has been finalised (noting any short-term compliance requirements). Identity documents should not be recoverable after deletion.

3.2. Implement audit controls that record what identity documents have been verified and a date/time stamp of when verifications occurred. For more information, go to Principle 4: Retain metadata only.

3.3. DSPs should engage third-party entities that provide identity verification services that have implemented points 3.1 and 3.2 and confirm their compliance with these through contract clauses and audit logs.

3.4. Provide notices and/or education material to customers and users to delete any identity verification documents once a verification process is completed.

Example 1: Identity verification, session timeouts and deletion

A software user issues an invitation for a client to complete their onboarding journey, which includes an identity verification step. The client starts the process but does not complete it within the timeframe set by the software (for example, within 24 hours). Once the session has expired, the software should automatically delete all captured information and identity documents.

There may be limited circumstances in which business processes (for example, risk and compliance team investigations into failed verification or multiple verification attempts) require retaining identity documents for a short period.

DSPs may consider supporting these processes for their customers or end users and providing a limited timeframe during which certain identity documents remain available for review (for example, 48 hours), after which they are deleted.

Example 2: Identity verification in employee hiring and onboarding

An employer uses a human resources (HR) platform to support their hiring process, which enables the employer to verify the identities of applicants during the application process.

The applicant's identity documents used for verification are retained within the HR platform to support the interview process and confirm that the individual attending the interview is the same person who applied for the job.

Similarly, employers may want to reverify the successful applicant during the employee onboarding process to ensure that the individual who was interviewed is the same one being onboarded.

The HR platform should immediately delete identity documents collected in this process after the following events occur:

- The individual does not proceed to the interview stage.
- The individual does not proceed after the interview stage.
- The individual has been hired, and onboarding with the employer is complete. Only a metadata record of identity verification is retained.

This principle relates to the following Australian (APP) and New Zealand (IPP) privacy principles:

- APP 3: Collection of solicited personal information
- APP 11: Security of personal information
- IPP 1: Purpose of collection of personal information
- IPP 9: Retention of personal information.

Principle 4: Retain metadata only

DSPs and their customers should only retain the minimum data required to demonstrate that an identity verification occurred for customer record-keeping purposes.

DSPs should only retain the following metadata for an identity verification result record:

- User identification of the person being verified
- Document type used to perform verification (for example, a passport or a driver's licence)
- Verification method (digital or visual)
- Unique system-generated verification number, Australian Document Verification Service (DVS) virtual reference number, or verifier identifier
- Verification timestamp.

Example 3: Digital identity verification

The following metadata should be retained:

- John Smith
- Passport
- Digital
- DA00110090871782
- 2021-01-28T23:45:00.000000Z

Example 4: Digital identity verification using DVS

The following metadata should be retained:

- Jane Smith
- Passport
- Digital
- Virtual Reference Number (DVS generated)
- 2021-01-28T23:45:00.000000Z

DSPs may also consider including a "reverification required date" to support customers with any ongoing verification requirements. Customers or end users may be able to configure this date to reflect their requirements (for example, 12 months, 24 months, or 36 months).

Storing only metadata enables DSPs to support customers in proving that a verification event occurred without retaining any identity documents.

Best Practice Guidance

4.1. Update data models to capture minimum identity verification metadata (as described above) and exclude document numbers, images, or scanned copies of identity documents.

This principle relates to the following Australian (APP) and New Zealand (IPP) privacy principles:

- APP 10: Quality of personal information
- APP 11: Security of personal information
- IPP 8: Accuracy of personal information
- IPP 9: Retention of personal information.

Principle 5: Protect verification data (security, audit, and assurance)

DSPs should protect all verification data with strong encryption, restrict access to this data to authorised system components or users, and maintain complete audit trails.

Limiting access to verification data in software prevents accidental exposure or misuse of this information. Encryption and audit processes protect sensitive information from unauthorised access and align with good governance practices, in line with Australian and New Zealand privacy principles.

Best Practice Guidance

5.1. Implement role-based access controls so only authorised system components or users can view verification data.

5.2. Retain verification data separately from other customer or operational data.

5.3. Use strong data in transit encryption standards, for example, TLS 1.3 or higher.

5.4. Use strong data at rest encryption standards, for example, AES-256.

5.5. Verification events should be logged, with the following events recorded:

- Any authorised or unauthorised attempts to access verification data
- Deletion events (including post-verification and other instances in software).

5.6. Conduct regular privacy and security testing.

This principle relates to the following Australian and New Zealand privacy principles:

- APP 6: Use or disclosure of personal information
- APP 11: Security of personal information
- IPP 5: Storage and security of information
- IPP 10: Limits on use of personal information
- IPP 11: Disclosure of personal information.

Principle 6: Be transparent with users

DSPs should clearly inform customers and end users about how identity documents are handled in software, highlighting:

- Copies of identity documents should not be uploaded and stored within software.
- Identity documents used to support verification processes are deleted, regardless of the outcome.
- Only metadata related to successful identity verification is retained within software.

DSPs should support customers by providing educational materials outlining how the risks associated with identity verification are mitigated and the steps customers can take to further reduce their exposure to breaches.

Best Practice Guidance

6.1. Provide user notices within software processes to inform customers that identity documents are deleted automatically after a verification event, and only metadata is

retained.

6.2. Include information in privacy policies and software terms and conditions about how identity documents are handled.

This principle relates to the following Australian and New Zealand privacy principles:

- APP 1: Open and transparent management of personal information
- APP 5: Notification of the collection of personal information
- IPP 3: Collection of information from subject - what to tell the individual
- IPP 6: Access to personal information.

Examples of Meeting Best Practice Principles

The following two examples demonstrate how DSPs can follow the best-practice principles outlined in this guidance.

Example 5: A DSP using a digital identity solution

A DSP integrates a third-party digital identity provider into its onboarding workflow. Customers complete identity verification through the provider's app. The DSP never directly handles identity documents; it only receives a verification result and associated metadata.

How the principles apply:

- **Principle 1: Enable digital-first identity verification**
  The DSP uses a third-party digital identity solution as the default verification method, reducing any need for physical document handling.
- **Principle 2: Prevent the upload or storage of identity documents**
  As all verification occurs through the digital identity provider, identity documents never enter the DSP's system. The DSP should still block document uploads in other areas of its product.
- **Principle 3: Delete identity documents after verification**
  The digital identity provider is responsible for deleting documents after verification. The DSP should still block document uploads in other areas of its product.
- **Principle 4: Retain metadata only**
  The digital identity provider sends the metadata associated with the verification to the DSP; the DSP stores it against the verified individual's account.
- **Principle 5: Protect verification data (security, audit, and assurance)**

The DSP secures metadata using best-practice encryption standards, applies role-based access controls, and maintains audit logs.

- **Principle 6: Be transparent with users**
  The DSP informs users that identity documents are not uploaded to or stored in the DSP's software and that only metadata is retained.

Example 6: DSP supporting in-person sighting

A DSP allows customers to conduct an in-person sighting of an identity document. The verifier visually checks the document and records the verification event in the DSP's software. The software does not allow upload, capture, or storage of identity documents.

How the principles apply:

- **Principle 1: Enable digital-first identity verification**
  Digital identity verification remains the preferred option, but in-person sighting is supported only where digital options are unavailable or impractical.
- **Principle 2: Prevent the upload or storage of identity documents**
  The software blocks any attempt to upload identity documents and provides guidance to customers that documents cannot be stored.
- **Principle 3: Delete identity documents after verification**
  No documents are captured, so deletion is not required.
- **Principle 4: Retain metadata only**
  The DSP stores only the verification metadata entered by the customer, such as:
  - Document type sighted
  - Verification method ("visual")
  - Verifier identifier (e.g. the natural person conducting the sighting).
  - Verification timestamp

  No scanned copies, photos, or document numbers are recorded.
- **Principle 5: Protect verification data (security, audit, and assurance)**
  Metadata is encrypted, access is limited to authorised roles, and all verification events are included in audit logs.
- **Principle 6: Be transparent with users**
  The DSP clearly states that identity documents cannot be uploaded and that only metadata from the in-person sighting is stored.

Conclusion

DSPANZ and its members are committed to a **digital-first** approach to identity verification that removes the need to collect and store identity documents. This approach mitigates the risk of data breaches involving personal identity information, providing a secure and streamlined experience for individuals, businesses, and DSPs.

By following this guidance, DSPs demonstrate that they use privacy-driven, secure identity verification processes that support customers and users in meeting their compliance obligations.

DSPANZ recognises that the further adoption and widespread use of digital identity and verifiable credentials is set to reshape the future of identity verification and can fundamentally transform and automate how DSPs support these processes.

DSPANZ will provide additional resources to help DSPs operationalise these practices.

Appendix 1: Alignment

This guidance aligns with common legislative and regulatory requirements that may apply to DSPs or their customers on identity verification, information protection, and best practice security frameworks and requirements.

Jurisdiction	Legislation or Requirement	Core Alignment
Australia	• *Privacy Act 1988* (Cth) • *Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act* • OAIC Australian Privacy Principles • ATO agent client verification methods - recording client verification	• Collection limitation • Destruction • Purpose limitation
New Zealand	• *Privacy Act 2020* • Department of Internal Affairs (DIA) Digital Identity Guidance	• Limited collection • No retention of unnecessary identifiers
Industry Context	• ATO DSP Operational Security Framework	• Secure, privacy-centric data handling aligned with API and software best practices

Appendix 2: Glossary

Term	Definition
API (Application Programming Interface)	A connection that allows software systems to communicate or share data automatically.
AML/CTF (Anti-Money Laundering and Counter-Terrorism Financing)	Laws requiring businesses to verify customers and prevent misuse of financial systems.
DSP (Digital Service Provider)	An organisation that develops or provides software to support accounting, payroll, and tax compliance.
DVS (Document Verification Service)	A service that checks whether the biographic information on your identity document matches the original record. More details on the DVS and gateway service providers can be found on the Australian Government's IDMatch website.

Identity Verification	The process of confirming that an individual is who they claim to be by validating information or credentials against trusted data sources.
Metadata	Information that describes a record (e.g. date, type) without revealing personal data.
TLS/AES Encryption	Security methods used to protect data during transmission (TLS) and at rest (AES).

Appendix 3: Digital Identity Working Group

The DSPANZ Digital Identity Working Group has developed this best practice guidance in collaboration with industry and government partners. More information about the working group, including its members, meeting materials, and other documents supporting this best practice guidance, can be found on the DSPANZ website.