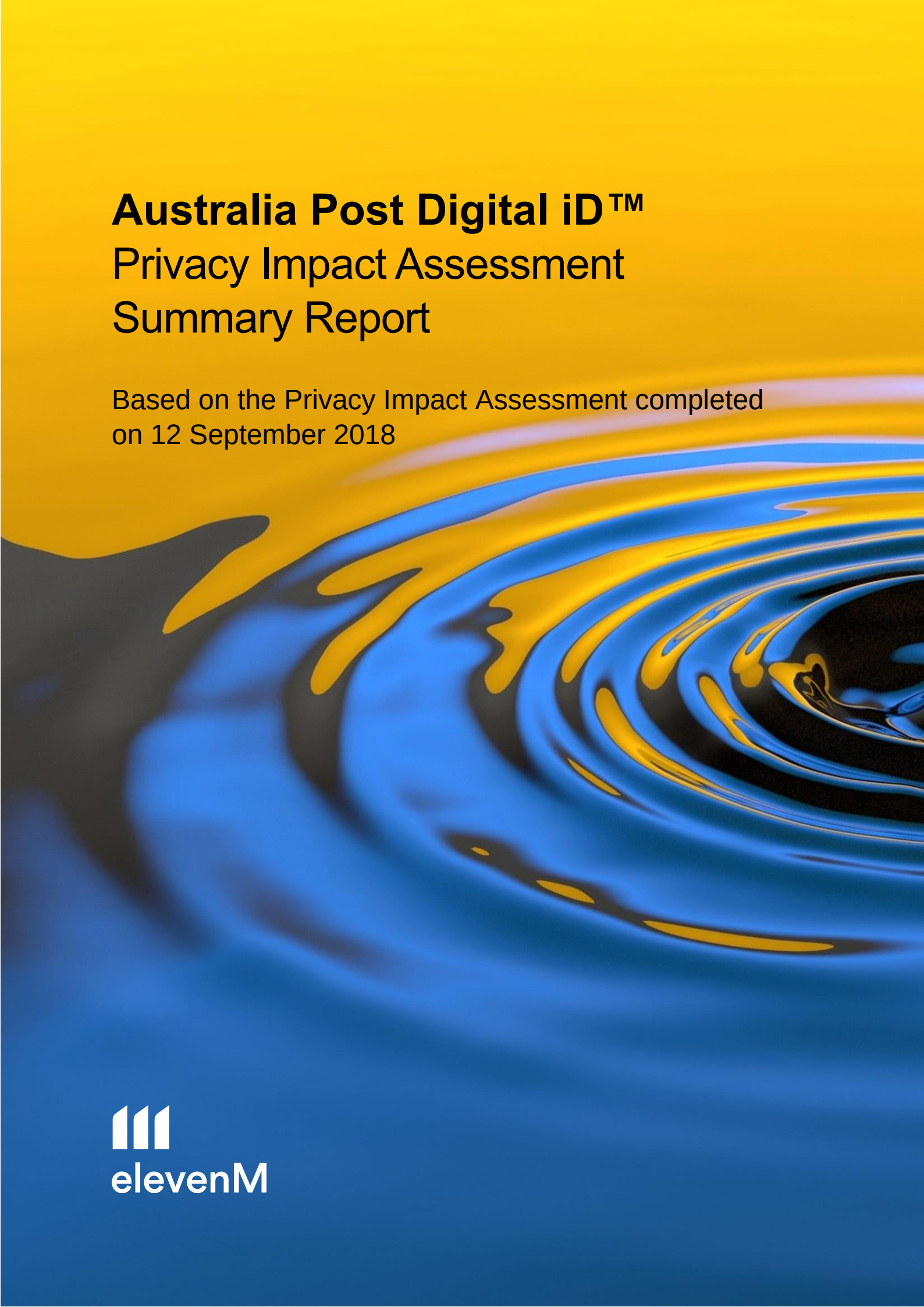
Australia Post Digital iD™
Privacy Impact Assessment Summary Report

Based on the Privacy Impact Assessment completed on 12 September 2018



elevenM

Background

Digital iD™ is a service that allows users to prove their identity with Australia Post and participating third parties. Australia Post is taking steps to obtain accreditation as an Identity Service Provider under the Trusted Digital Identity Framework (**TDIF**), which is administered by the Trust Framework Accreditation Authority (**TFAA**).

Australia Post engaged elevenM to carry out a Privacy Impact Assessment (**PIA**) in relation to the Digital iD™ product. The Digital iD™ PIA was completed on 12 September 2018 and this summary report was subsequently completed on 2 August 2019.

About Digital iD™

The Digital iD™ service allows individuals to prove their identity electronically with Australia Post, and to reuse their verified identity across participating third parties (**counterparties**). Users can build up the strength of their identity by verifying documents including passports, driver licences and Medicare cards. Digital iD™ users can also add a verified photo of themselves to their profile and display it using the Digital iD™ app.

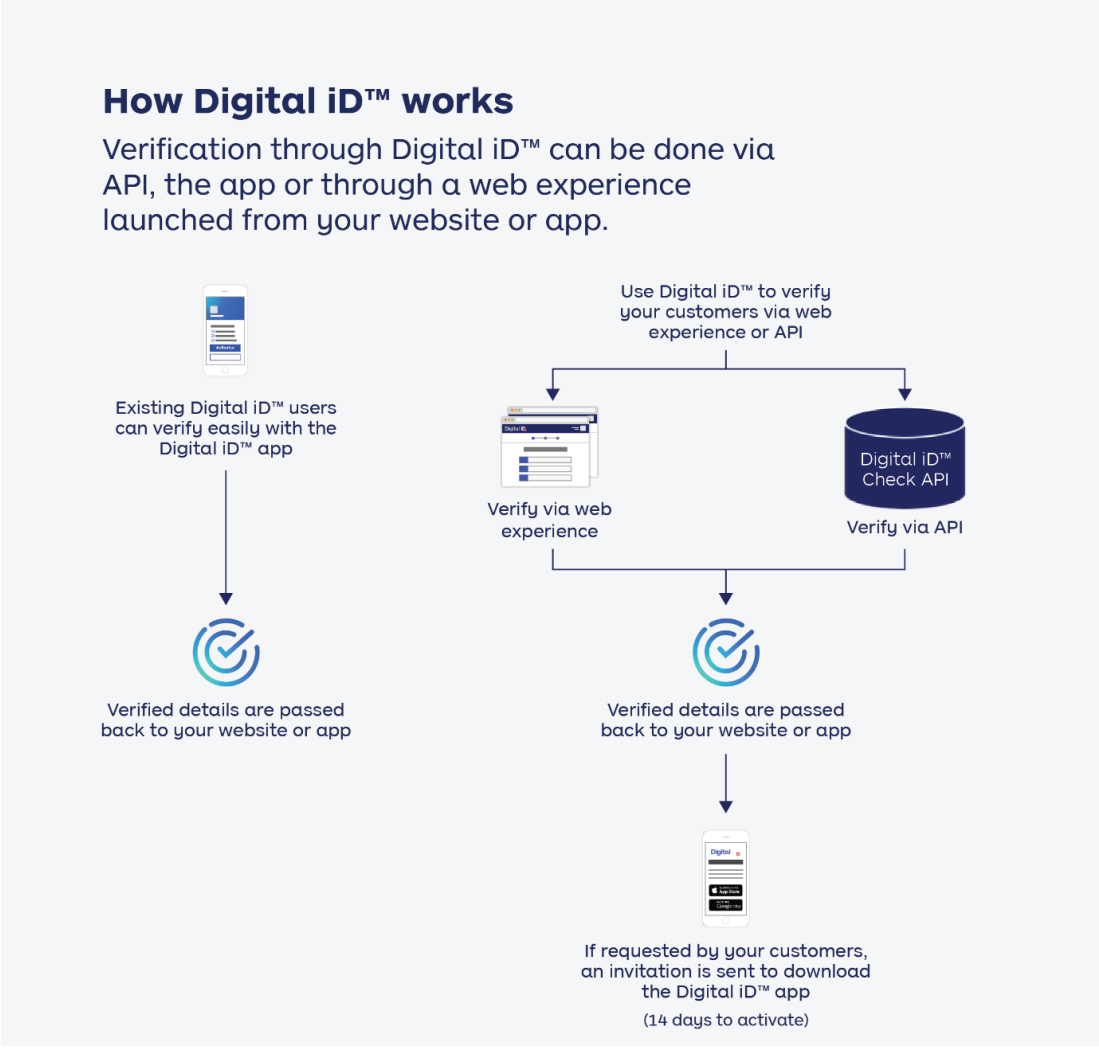


Figure 1: Illustration of the Digital iD™ system from a counterparty perspective

Digital iD™ can be accessed by individuals through a web-based interface or via a mobile app. A user's Digital iD™ is bound to their mobile device, with a phone number used for initial registration. Any identity information provided by the user is stored on Digital iD™ servers and encrypted using a public key held by Digital iD™. The corresponding private key, which is required to decrypt a user's identity information, is stored on a user's mobile device and can only be accessed with the user's consent.

If a user deletes the Digital iD™ from their phone, the private key is lost and the user's identity information (stored on Digital iD™ servers) cannot be decrypted. If the user wishes to use Digital iD™ again, they must create a new profile and re-verify their identity information.

Figure 1 above illustrates how the Digital iD™ service works from the perspective of a counterparty. This diagram is a summary prepared by Australia Post and is not a comprehensive description of the flows of personal information throughout the Digital iD™ service.

The Digital iD™ PIA

The Digital iD™ PIA was delivered to Australia Post in September 2018. It documented flows of personal information associated with Digital iD™ and identified privacy risks and opportunities associated with:

- the Australian Privacy Principles (**APPs**) and, Notifiable Data Breaches Scheme (**NDBS**) under the *Privacy Act 1988* (Cth) (**Privacy Act**);
- the core Privacy Requirements (**CPRs**) which form part of the TDIF; and
- community expectations and privacy best practices.

The PIA's findings included 7 risks (with 11 resulting recommendations), 1 opportunity for improvement (with 1 resulting recommendation), and a further 3 general recommendations relating to best practice. In total, the PIA made 15 recommendations across the areas of privacy governance, the collection of personal information, dealing with personal information and the integrity of personal information.

The table below provides an overview of these findings.

Principle	Summary of findings
Privacy governance	
Open and transparent management of personal information	**Risk 1** (2 recommendations) – see page 5 **Risk 2** (2 recommendations) – see page 6 **Opportunity 1** (1 recommendation) – see page 6
Anonymity and pseudonymity	No findings

Principle	Summary of findings
Collection of personal information	
Solicited personal information	No findings
Unsolicited personal information	No findings
Notification of collection	**Risk 3** (2 recommendations) – see page 8
Dealing with personal information	
Consent management	**Risk 4** (2 recommendations) – see page 8
Use or disclosure	**Risk 5** (1 recommendation) – see page 10
Direct marketing	No findings
Cross-border disclosure	**3 general recommendations** – see page 10
Government-related identifiers	No findings
Integrity of personal information	
Quality of personal information	**Risk 6** (1 recommendation) – see page 12
Security of personal information	No findings
Data breach management	**Risk 7** (1 recommendation) – see page 14
Access to personal information	No findings
Correction of personal information	No findings

A summary of the analysis from the PIA, including the detail of each finding and its associated recommendations, is set out in the following section. Australia Post intends to publish its response to these recommendations on its website.

Summary of analysis

Privacy governance

	Summary of analysis	Findings & Recommendations
Open and transparent management of personal information	The Digital iD™ website (https://digitalid.com), Privacy Notice and Terms of Use describe in an open and transparent way how Australia Post will handle personal information while offering the service, and the Australia Post Privacy Policy is consistent with how Digital iD™ involves handling personal information. Publishing a suitable summarised version of the Digital iD™ PIA would build trust with users and position Australia Post as a responsible Identity Service Provider. Australia Post should proactively work with TFAA and other complaint handling bodies to reach agreement on a model for notifying/obtaining consent to the disclosure of personal information about individuals who make complaints. Generally, Digital iD™ will not negatively impact on Australia Post's ability to openly and transparently manage personal information, except possibly in the case of young users who may lack the capacity to understand the implications of disclosing their personal information.	**Risk 1:** Young individuals (under the age of 18) might use Digital iD™ without understanding how their personal information is being handled and without the capacity to give consent to its collection and use. This may lead to regulatory and reputational impacts for Australia Post and personal impacts for individuals. **Recommendations:** • Consider simplifying the Digital iD™ Privacy Notice and Terms of Use to reduce their effective reading age. Alternatively, adopt a simplified "tiered" Privacy Notice which summarises and links to key points in the standard Privacy Notice. • Consider adopting a "soft" age limit, below which users will be encouraged to seek help from a legally responsible adult (13 is a common minimum age limit for many online services and may serve as a suitable soft age limit). This would involve altering the profile creation flow to encourage users under 18 to seek help from their parent or guardian during setup.

	Summary of analysis	Findings & Recommendations
		Risk 2: Complaints handling staff may not have knowledge of the Trusted Digital Identity Framework and may not be equipped to appropriately direct complaints related to Digital iD™. **Recommendations:** • Ensure that Australia Post's complaints handling staff (or a subset) are trained to deal with complaints related to Digital iD™ and are familiar with the APPs and the Trusted Digital Identity Framework. • Work with the accreditation authority and other complaint handling bodies to reach agreement on an integrated complaint handling model, including a threshold for determining the adequacy of de-identification processes. **Opportunity 1:** Build user trust by publishing a summary of the findings in this PIA. **Recommendation:** • Prepare and publish a summary of this PIA after it has been finalised and resulting actions have been closed.
Anonymity and pseudonymity	It is not practicable to allow individuals to remain anonymous or to use a pseudonym when they use Digital iD's™ identity verification functionality.	No findings.

Collection of personal information

	Summary of analysis	Findings & Recommendations
Solicited personal information	To offer the Digital iD™ service, Australia Post collects name, date of birth, mobile phone number, residential address, selfie photograph and identity document details. This information is reasonably necessary for identity verification and AML check purposes. Australia Post collects biometric data when a user uploads a selfie or data scanned from an NFC-enabled passport (which includes passport photo). This biometric data is used to verify the individual's attributes. The selfie is retained by Australia Post in encrypted form for ongoing verification purposes. The passport photo is used to verify the user's selfie and is then destroyed. Australia Post only collects personal information directly from individuals through the Digital iD™ app or website.	No findings.
Unsolicited personal information	Individuals provide personal information through formal channels (i.e. the Digital iD™ app or website) to create a profile and verify their identity. There is a function on the website which allows users to submit their feedback to Australia Post and, in the past, some users have submitted unnecessary personal information using this form. Australia Post's Support Guide instructs staff to delete or redact this information. Digital ID's™ support processes mandate that all support toolsets, documents and other records must not contain personal information of users and users' personal information must not be requested, captured, recorded or retained during call centre interaction.	No findings.

	Summary of analysis	Findings & Recommendations
Notification of collection	Users are directed to the Digital iD™ Privacy Notice when consenting to their personal information being collected for the purpose of identity verification. Counterparties who collect personal information using Digital iD™ infrastructure are contractually required to notify individuals that their personal information will be disclosed to Australia Post for the purpose of identity verification. Australia Post obtains user consent before users can provide any personal information (including sensitive information). The TDIF requires Australia Post to inform users of alternative channels to verify their identity. This obligation is likely intended to apply to counterparties ("Relying Parties" under the TDIF), to promote competition and ensure that consumers have a choice of identity provider. While the Digital iD™ website, app, Privacy Notice and Terms of Use do not suggest that Digital iD™ is an exclusive method of electronic identity verification, there is no mention of alternative channels to verify user identity.	**Risk 3:** Australia Post may not comply with the Trusted Digital Identity Framework if it does not inform users that there are alternative channels for verifying their identity or of the consequences of declining to provide required information. **Recommendations:** • Confirm with the accreditation authority whether Identity Service Providers are expected to inform users of alternative channels for verifying their identity. • Subject to clarification and approval, consider adding information within the Digital iD™ Terms of Use to notify readers that Australia Post is an Identity Service Provider under the Trusted Digital Identity Framework, and that there are other providers operating within the framework.

Dealing with personal information

	Summary of analysis	Findings & Recommendations
Consent management	Australia Post provides a consent notice that is explicit, voluntary, current and specific when:	**Risk 4:** The transaction confirmation screen does not inform users that Australia Post will record the transaction (for storage in its audit

	Summary of analysis	Findings & Recommendations
	• a user's personal information is about to be collected; and • a user's personal information will be shared with a counterparty, (in which case they are shown the identity of the counterparty and the types of information that will be shared). The Privacy Notice informs users of the implications of withholding consent (although it is not displayed when consent to share is being sought). Users are not notified that Australia Post will record the transaction (for storage in its audit logs). This is technically a collection of personal information. Digital iD™ does not incorporate controls to ensure users have the capacity to understand and communicate their consent. It may be possible to impose a user age limit, but other measures for ensuring user capacity are likely to be impracticable. Each collection of personal information via Digital iD™ occurs on a one-off basis (i.e. collection is not ongoing) and is logged and stored by Australia Post to demonstrate that consent was obtained and is current. There is currently no process for individuals to withdraw their consent to Australia Post holding personal information which it previously collected. However, Australia Post is technically incapable of reading the data without consent from individuals. By deleting the Digital iD™ app from their phone, individuals render the identity information held on Digital iD™ servers effectively unreadable (and unrecoverable).	logs). This is technically a collection of personal information. **Recommendations:** • Enhance the transaction confirmation screen with additional privacy information. At a minimum, include a note indicating that the transaction will be recorded by Australia Post and displayed in the record of the user's past activity, with a link to the Privacy Notice. For example, the "Allow" button could be amended to state: "Allow and save in activity feed", with a link to the Privacy Notice displayed elsewhere on the screen. • Consider also allowing counterparties to embed a link to their privacy collection statement in this screen.

	Summary of analysis	Findings & Recommendations
Use and disclosure	The Digital iD™ app and website require user consent before a user's personal information can be accessed by Australia Post or shared with a counterparty. Because of the solution's design, Australia Post is not able to access identity verification information without individual user consent. Australia Post does not propose to use personal information handled as part of the Digital iD™ service for any secondary purpose beyond information verification and related administrative uses. Australia Post may use some existing personal information from mail redirection and parcel manifest for verifying user identities – users will be required to consent to this use, as it is a secondary use of the personal information. Once Australia Post discloses personal information to a counterparty, it loses effective control over the copy of the information. A counterparty using information in a manner contrary to user expectations carries an associated reputational risk for Australia Post. Australia Post can currently assess counterparty risks on a case-by-case basis, however, to enable a large volume of counterparties to access Digital iD™, Australia Post intends to develop a self-service onboarding process in the future which will require a principles-based framework for reviewing and identifying issues associated with counterparties and how they use the personal information available through Digital iD™.	**Risk 5:** Australia Post and Digital iD™ may suffer reputational damage if a counterparty uses personal information collected through Digital iD™ for a secondary purpose or in a manner that contradicts community expectations. **Recommendation:** • Before deploying a self-service onboarding process for counterparties, establish a framework for managing counterparty risk which identifies categories of appropriate and inappropriate uses of identity information.
Direct marketing	Australia Post does not intend to use the personal information it collects using Digital iD™ for any form of direct marketing.	No findings.
Cross-border disclosure	Australia Post does not currently disclose any personal information handled as part of the Digital iD™ service to recipients outside of	**General recommendations:** • When establishing the standard terms for counterparties outside of Australia, ensure

	Summary of analysis	Findings & Recommendations

	Australia. As such, it does not currently have a standard form agreement for use with counterparties outside of Australia.
	
	The current version of the standard agreement between Australia Post and counterparties requires counterparties to warrant that they are subject to the Privacy Act as an APP entity and that personal information collected through Digital iD™ may only be used for identity verification purposes.
	
	Should Australia Post onboard counterparties outside of Australia or that are otherwise not APP entities under the Privacy Act, it will need to ensure these counterparties adopt privacy practices at least substantially similar to those under the APPs and agree that personal information collected through Digital iD™ may only be used for identity verification purposes.
		that counterparties are contractually required to adopt privacy practices at least substantially similar to those under the APPs.
		
		• When establishing the standard terms for counterparties outside of Australia, ensure that counterparties may only use personal information collected through Digital iD™ for identity verification purposes.
		
		• When establishing the standard terms for counterparties outside of Australia, ensure that the agreement with the counterparty specifies:
		  ○ why the counterparty may handle the personal information;
		  ○ the minimum technical and organisation protections applying to the information;
		  ○ that Australia Post can require the counterparty to destroy the information; and
		  ○ mechanisms for monitoring compliance with the contract,
		among any other requirements imposed under the CPRs.

Adoption, use and disclosure of government	Australia Post collects government related identifiers as part of the identity verification process and transmits these identifiers to third-party verification sources.	No findings.

	Summary of analysis	Findings & Recommendations
related identifiers	Australia Post will not disclose government related identifiers to counterparties. If a counterparty requests a government related identifier, Australia Post follows a standard process to determine that the counterparty is eligible to receive the identifier. Australia Post creates a new internal identifier to track against each Digital iD™ profile, but this is not intended to serve as a unifying identifier for use across the TDIF ecosystem and is not shared with counterparties.	

Integrity of personal information

	Summary of analysis	Findings & Recommendations
Quality of personal information	Identity information is collected directly from individuals and confirmed using third-party verification sources which ensures it is accurate, up-to-date, complete and not misleading at the time it is collected. This information is collected for the purposes of a digital identity service. Digital iD™ recognises expired identity documents and will not allow their contents to be shared with counterparties, but if a user has changed their name or address, the previously entered information (now out of date) will be shared with counterparties. Digital iD™ does not allow users to update their personal details – instead the users must delete the app and create a new profile with their current details, but any past transaction history will be lost.	**Risk 6:** Potential non-compliance with the Trusted Digital Identity Framework by not allowing individuals to update their personal information without deleting and creating a new profile. **Recommendation:** • Consider allowing users to upload new identify verification at any time, even if they have already provided the same type of information. For instance, a user who has replaced a lost passport may wish to update their information to include the details of the new document without having to delete the app and re-register. This would not require

	Summary of analysis	Findings & Recommendations
	The benefit in allowing users to directly update information may be outweighed by the additional complexity this functionality would add to the product. Australia Post carries out verification procedures whenever a user adds new identity information to their Digital iD™ profile. However, it does not monitor for outdated or incorrect information following collection, as this would require user consent to access the contents of identity documents. Australia Post immediately adds any new personal information it collects from a Digital iD™ user to the user's records. The Digital iD™ app allows users to view the types of identity documents that they have uploaded and verified but not to view the data extracted from these documents (e.g., the passport number). On balance, it is reasonable not to display this information to users as Digital iD™ is not intended to serve as an identity "wallet", allowing users to view their identity information at any time. There are security reasons for preventing access to this information. Users cannot remove previously verified documents.	Australia Post to display the previously provided information, nor to proactively check for its currency.
Security of personal information	Digital iD™ was developed according to Australia Post's secure development lifecycle, which required security reviews at specific stages of the development process. Security penetration testing has been carried out continuously in relation to the Digital iD™ app, website and backend systems. Australia Post encrypts all data consumed by the Digital iD™ service both in transit and at rest. Australia Post staff can access some basic profile information (e.g. mobile phone number) which is used for administrative purposes and to enable notifications to be sent to users. However, the Digital iD™ system	No findings.

	Summary of analysis	Findings & Recommendations
	architectures means that identity verification information cannot be accessed without a user's private key which can only be provided from the Digital iD™ app with the user's consent. All access to Digital iD™ data is monitored and logged. Australia Post has written management policies concerning retention timeframes across all business records it maintains. Australia Post's IT solutions team implements deactivation policies and practices and associated destruction processes. Information around enterprise retention practices are provided on the Australia Post intranet, accessible by all corporate staff. There is also a dedicated resource who works with the business to ensure applicable timeframes are applied.	
Data breach management	The TFAA requires Australia Post to notify the OAIC, affected individuals and the TFAA of data breaches that are likely to result in serious harm to individuals (and which have not been effectively remediated). This does not extend Australia Post's requirements under the Notifiable Data Breaches Scheme (NDBS) except that the TFAA must also be notified in the case of an eligible data breach.	**Risk 7:** Failing to notify the Trust Framework Accreditation Authority in the case of a data breach **Recommendation:** • Update Australia Post's Data Breach Response Plan to incorporate a test to determine whether a breach involves personal information handled as part of Digital iD™, and instructions for notifying the TFAA.

Access to, and correction of, personal information

Note: Considerations relating to access to personal information and correction of personal information have been combined for the purposes of this PIA summary.

	Summary of analysis	Findings & Recommendations
Access to, and correction of, personal information	Australia Post will rely on manual processes for providing access to personal information which users have requested. Some information (for example, the types of identity documents that users have uploaded and verified) will be viewable by users on the Digital iD™ app. However, users cannot view the data extracted from these documents. Information requests in relation to Digital iD™ are handled using Australia Post's existing information request processes.	No findings.