Commonwealth Digital Transformation Agency (DTA)

Initial Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework (TDIF) Alpha

FINAL

5 December 2016

(GC460)

Contact: Galexia
Ph: +61 2 9660 1111
www.galexia.com
Email: dta@galexia.com

Contents

1. Executive Summary

1.1. Approach and Scope

Galexia <www.galexia.com> has completed this initial Privacy Impact Assessment (PIA) for the Digital Transformation Agency (DTA) <www.dta.gov.au> on the proposal to establish a Trusted Digital Identity Framework (TDIF).

This initial PIA is the first step in a multi-phase and independent PIA process commissioned by the Digital Transformation Agency, incorporating:

1. An initial PIA on the overall concept and design of the Trusted Digital Identity Framework (TDIF) and some of its key components (November 2016);
2. A full PIA on the planned implementation of the Trusted Digital Identity Framework (TDIF) and some of its key components (estimated March 2017); and
3. Individual PIAs for each Identity Provider (IdP) that applies to be accredited under the Trusted Digital Identity Framework (TDIF) (as required); and
4. Individual PIAs for other accredited TDIF Participants (such as the Identity Exchange, Attribute Providers and Credential Providers) (as required).

This initial PIA has been conducted in accordance with *PIA Guidelines* issued by the Office of the Australian Information Commissioner.

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by the broad concept and design of the overall Trusted Digital Identity Framework (TDIF) and some of its components. The key components are:

1. The proposed development of mandatory standards, policies and agreements for all TDIF participants;
2. The proposed development of an Identity Exchange; and
3. The proposed development of a Commonwealth Identity Provider (IdP).

Each of the components raises different privacy issues.

This PIA considers compliance with privacy legislation, user acceptance and public perception issues. As it is an initial PIA on the high level concept and design, the PIA makes a broad range of recommendations for mediating privacy risks, including changes to the design, practical privacy compliance steps, further research and privacy governance arrangements.

It is important to note that the scope of this PIA is limited to Commonwealth agencies operating under the Commonwealth privacy law framework. Other state and territory agencies (and private sector organisations) may seek to join the TDIF, subject to a further detailed review of privacy issues relevant to each entity. The proposed TDIF Core Service Requirements envisage that a new PIA would be conducted for each agency or organisation joining the TDIF.

Information contained in this PIA is based on:

- Meetings with the Digital Transformation Agency (DTA), including senior management, technical staff, policy staff and relevant contractors;
- A series of telephone and face-to-face meetings with key stakeholders (further details *included Section 21. Appendix 1 – Stakeholder Consultation*);
- Documentation related to the proposal (further details in *Section 22. Appendix 2 – Background Information*)
    - Trusted Digital Identity Framework (TDIF) Documentation Stack (as at August 2016)
        - Overview
        - Digital Identity Risk Management Standard
        - Digital Identity Verification Standard
        - Digital Authentication Credential Standard
        - Core Service Requirements (CSR)

        - Federated Identity Architecture
        - Memorandum of Agreement Template
        - Glossary of Terms
    - Digital Identity – Individuals (Architecture)
- Two round table meetings between the DTA and stakeholders:
    - Digital Transformation Roundtable, Authentication and Verification 'Deep Dive', 25 October 2016, Sydney; and
    - State & Territory Government Stakeholders Meeting, 10 November 2016, Sydney
- Review of an early demonstration prototype of GovPass – the provisional name for the consumer facing elements of the TDIF;
- General research and literature review on privacy and identity verification issues; and
- Review of relevant privacy legislation and guidelines.

Galexia's advice in this PIA concentrates on the following areas:

- **Commonwealth Privacy Act compliance**
  This PIA assesses the proposed implementation of the Trusted Digital Identity Framework (TDIF) against the Australian Privacy Principles (APPs) in the Commonwealth Privacy Act. This assessment is mainly relevant to the Commonwealth agencies involved in the TDIF, but provides a useful 'structure' for considering privacy issues that apply to other participants.
- **Practical measures to address privacy**
  This PIA identifies several practical measures that can be taken to manage privacy issues, including proposed changes to the design and suggested content for the TDIF Core Service Requirements;
- **Governance**
  The PIA considers key privacy governance steps that could be implemented to ensure the ongoing protection of privacy once the TDIF and its components are operational, including advice on structural separation, ongoing evaluation and oversight arrangements;
- **Future work plan**
  This PIA has identified several priority tasks to be included in the DTA future work plan.

The PIA includes recommendations for action by the DTA as summarised in the following sections. It is important to note that the recommendations are designed as a 'package' to manage the overall privacy impact of the design and implementation of the TDIF.

The DTA has reviewed the draft PIA and has been closely engaged in the PIA process. Some of the PIA recommendations already form part of the DTA work plan for the TDIF.

1.2. TDIF Privacy Issues Summary

Each of the TDIF components raises slightly different privacy issues. This PIA follows the Commonwealth PIA Guidelines, so each section examines compliance against a specific APP (refer to section 1.3 below). However, it is also useful to examine the *overall* privacy issues facing each TDIF component, as summarised in the following table:

TDIF Component	Status	Galexia Commentary	Recommendation
1. Mandatory policies and standards	**Requires further review / action**	The first key component of the TDIF is the proposed development of mandatory standards, policies and agreements for all TDIF participants. As these policies and standards are mandatory, there is the potential that the TDIF will drive an improvement in the implementation of digital identity in Australia. TDIF participants will be evaluated against the standards at the time of application, and then on an ongoing basis (through a series of regular audits). They risk having their accreditation revoked if their processes and practices fail to meet the standards. In turn, the standards include some sections on privacy and security (in the TDIF Core Service Requirements), although the details of these requirements are yet to be developed. Overall, these arrangements would appear to be positive for the protection of privacy, and they received favourable comments from many stakeholders during the consultations for this initial PIA. However, the PIA makes some minor recommendations in relation to this component.	**R1: The TDIF Membership Accreditation / Revocation Proposal** The development of the TDIF membership proposal, including accreditation and revocation, would benefit from significant further work on developing the detailed provisions and legal backing / powers / national agreement for the proposal, followed by further consultation with stakeholders. Stakeholders currently have very low expectations that this aspect of the TDIF can be developed or enforced. **R2: Privacy Principles in the Core Service Requirements** The DTA should consider the full range of options for incorporating privacy principles in the TDIF Core Service Requirements). The strengths and limitations of each option should be considered side by side, and discussed with key stakeholders. This discussion would benefit from the development of draft principles that attempt to set the highest possible standard based on existing laws in each jurisdiction, but this option should not be the only option available for discussion. Practical issues for the implementation of each option should also be considered, and solutions proposed.
2. The Identity Exchange	**Requires further review / action**	The Identity Exchange includes elements that are designed to minimise the amount of personal data that is collected and stored, to 'blind' IdPs and relying parties from information about the detailed use of identities, and to provide consumers with choice about which identity they use in each transaction. All of these elements were clearly recognised by stakeholders as being privacy positive. However, stakeholders did express concerns related to the collection, use and disclosure of metadata by the Identity Exchange.	**R3: The Identity Exchange and the retention of metadata** DTA should conduct further research on the period that meta-data needs to be retained in order to facilitate the investigation of identity fraud and suspicious transactions. This period should then be 'balanced' against the privacy risks and impacts of retaining the data, and an appropriate data retention period should be incorporated into the design of the Identity Exchange. For the avoidance of doubt, an 'appropriate period' could be shorter than the period required for all investigative purposes.

TDIF Component	Status	Galexia Commentary	Recommendation
3. Identity Providers (IdPs)	**Requires further review / action**	IdPs play an important role in the TDIF. The entire model is built on multiple IdPs operating, with stakeholder expectation that there will be IdPs at the Commonwealth level, at least some State and Territory IdPs and potentially some private sector IdPs. At the Commonwealth level, the DTA has decided to develop a single IdP. Existing Commonwealth digital identities will be transitioned to the Commonwealth IdP, and no further IdPs will be allowed to develop at the Commonwealth level. In contrast to the Identity Exchange, IdPs do collect and store significant amounts of personal data. The proposals relating to IdPs are the subject of significant privacy concerns from stakeholders.	**R4: The selection of a single Commonwealth IdP – further consultation** The DTA should recognise stakeholder concerns regarding the decision to establish a single Commonwealth IdP and should take steps to ensure that the proposal has an appropriate level of stakeholder and community understanding and support before implementing the proposal. **R5: The selection of a single Commonwealth IdP – Risk Assessment** The DTA should commission an independent risk assessment of the proposal to establish a single Commonwealth IdP, in comparison to the risks of other options, to ensure that the consequences of the proposed model do not represent an unacceptable risk to the community.

1.3. Australian Privacy Principle (APP) Compliance Summary

This PIA assesses the proposed implementation of the TDIF against the APPs in the Commonwealth Privacy Act. This assessment is mainly relevant to the Commonwealth agencies participating in the TDIF, but provides a useful 'structure' for the consideration of privacy issues that will be relevant to all participants.

The following table summarises the main findings, with links to further information and detailed discussion in the text:

Australian Privacy Principle (APP)	Status	Galexia Commentary	Recommendation
Is the data 'personal information'?	**Requires further review / action**	In the case of the TDIF this PIA concludes that all data collected, stored and used by Identity Providers (IdPs) should be classified and treated as Personal Information under the Privacy Act. This PIA also concludes that all data collected, stored and used by the Identity Exchange should be classified and treated as Personal Information under the Privacy Act.	**R6: Identity Providers and the definition of Personal Information** All data collected, stored and used by Identity Providers (IdPs) should be classified and treated as Personal Information. **R7: The Identity Exchange and the definition of Personal Information** All data collected, stored and used by the Identity Exchange should be classified and treated as Personal Information.

Australian Privacy Principle (APP)	Status	Galexia Commentary	Recommendation
APP 1 – Openness and Transparency	**Requires further review / action**	APP 1 (or its TDIF equivalent) will apply to all TDIF participants. Compliance should not present any difficulties, and participants need to develop or amend their public privacy principles to explain the operation of the TDIF and its impact.	**R8: Openness task** Specific requirements on openness and transparency should be set out in the TDIF Core Service Requirements. • IdPs will be required to develop a stand-alone privacy policy and submit it as part of their TDIF application. • Relying Parties will need to amend or expand their existing privacy policies to incorporate references to key data collection, use and disclosure that is facilitated by the TDIF. • The Identity Exchange will need to develop a stand-alone privacy policy.
APP 2 – Anonymity and Pseudonymity	**Compliant**	The TDIF is an identity framework designed to cater for transactions that require Level 2 and Level 3 identity.[1] There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level.	While not limiting or downplaying the requirement for agencies to provide anonymous and pseudonymous options to consumers in appropriate transactions and services on a case-by-case basis, APP 2 is not relevant to the TDIF, and is not the subject of detailed consideration in this PIA.
APP 3 – Collection of solicited personal information	**Requires further review / action**	The TDIF Core Service Requirements should include a collection principle and sub-principles (that ensure collection is necessary, that collection only occurs by lawful and fair means, and that collection is from the individual concerned). One item related to collection that requires further review is the collection of sensitive information. In the APPs this requires specific and explicit consent. In the TDIF this may be relevant because some IdPs may be collecting biometric information during enrolment. In the demonstration prototype users are asked to submit a photograph of their face – a biometric 'template' is created based on this photograph and then checked against the FVS. Although the photograph is not retained, this process should be considered a collection of biometric data.	**R9: Collection of sensitive data** The next iteration of the TDIF design will need to incorporate a request for specific explicit consent from users to the collection of biometric data. This occurs at the enrolment stage. The project would benefit from some further user testing regarding whether users understand the consent that they are providing in relation to the collection of biometric data.
APP 4 – Dealing with unsolicited personal information	**Compliant**	It is difficult to see how unsolicited information might be received by participants in the TDIF. However, it is impossible to rule this out, and APP 4 requires agencies and organisations to assess unsolicited information as it arrives, and destroy it if it is information that they could not have collected themselves.	This principle on unsolicited information is not usually included in other privacy laws – it is unique to the Commonwealth APPs. However, it is likely that this principle will need to be incorporated into the TDIF Core Service Requirements.

[1] The TDIF incorporates 'assurance levels' that are designed to reflect the risk profile of transactions undertaken using digital credentials.

Australian Privacy Principle (APP)	Status	Galexia Commentary	Recommendation
APP 5 – Notification	Requires further review / action	The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles. The principles will definitely include notice requirements. The content of the notices will need to be determined during the full PIA (2017).	**R10: Notice requirements** Notice will need to be provided by: • IdPs – at the time they enrol individuals and again when individual log in to the service to manage their identities or make an inquiry; • Relying Parties – at the time they refer consumers to the Identity Exchange; and • The Identity Exchange – at the time consumers visit the Exchange to select an IdP for enrolment, and again at the time they visit the Exchange to select an IdP for authentication.
APP 6 – Use or Disclosure	Requires further review / action	The TDIF is in the early stage of development, and an initial PIA limited to a high level review of the concept and design of the TDIF and its core components. At this early stage it is difficult to provide detailed advice on compliance with APP 6, but we can point to some key privacy issues that will be relevant to the TDIF. Three key issues are: • Secondary use for investigating identity fraud, • Use of biometric data and the • Development of a transparency report regarding law enforcement access.	**R11: Secondary use for investigating identity fraud and suspicious transactions** The exact scope and rules for the investigation of identity fraud and suspicious transactions by TDIF participants should be addressed in the TDIF Core Service Requirements and other TDIF documentation. The extent of this secondary use should be disclosed to consumers. **R12: Use of biometric data** APP 6 provides some additional rules for the use and disclosure of biometric data. However, the detailed provisions are delegated to 'guidelines' which have not yet been developed. In the meantime, the TDIF Core Service requirements should incorporate some additional privacy protections for the use of biometric data in the TDIF. These should include (at least): A. A strict prohibition on the biometric data being used for any secondary purpose (i.e. it would be restricted to verification of a photograph during initial enrolment); B. A requirement for all biometric data to be destroyed once the photograph has been verified; and C. The extension of these rules to all TDIF participants (APP 6.3 only applies to government agencies). **R13: Development of a transparency report** APP 6 requires entities to keep a written note of third party access to data by law enforcement agencies. This is an area where the TDIF Core Service Requirements could help to strengthen privacy protections,

Australian Privacy Principle (APP)	Status	Galexia Commentary	Recommendation
			beyond the very limited requirements in the Privacy Act. Emerging best practice is for organisations to issue annual 'transparency reports' that disclose the broad scale and scope of access requests by law enforcement agencies. The TDIF should adopt this approach and publish a regular transparency report.
APP 7 – Direct Marketing	**Requires further review / action**	The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles. Under either option, the use of TDIF personal data for direct marketing should be prohibited.	**R14: Direct marketing prohibition** The use of TDIF personal data for direct marketing should be prohibited in the TDIF Core Service Requirements.
APP 8 – Cross Border Disclosure	**Requires further review / action**	The TDIF should insist on a single approach to protecting privacy in the case of cross border data transfers. This approach should be set out in detail in the TDIF Core Service requirements, following further consultation with stakeholders.	**R15: Cross border data transfer – Mapping** Each TDIF participant should identify and map their cross-border data transfers. This is an important step in meeting the (expected) notice and protection provisions in the TDIF Core Service Requirements **R16: Cross border data transfer – Protection** Cross border data transfers in the TDIF should be permitted subject to the development of a single, consistent mechanism for protecting privacy in such transfers. The protection mechanism should be included in the TDIF Core Service Requirements. For the avoidance of doubt the protection mechanism could be both stronger and less flexible than the approaches permitted in current privacy law (particularly APP 8 in the Commonwealth Privacy Act), in order to meet the objective of consistent privacy protection throughout the TDIF.

Australian Privacy Principle (APP)	Status	Galexia Commentary	Recommendation
APP 9 – Government Related Identifiers	**Further action required**	The TDIF will result in IdPs developing new identifiers in order to uniquely identify their clients. APP 9 does not provide a sufficient level of privacy protection in relation to these identifiers. The TDIF Core Service requirements should therefore be strengthened to incorporate additional protections in relation to IdP identifiers.	**R17: Restriction on the use of IdP identifiers** Unique identifiers developed by IdPs should not be adopted by any third party as their identifier and the disclosure of IdP identifiers should be severely restricted to specific situations requiring verification of identity. **R18: Additional restriction on IdP identifiers** In order to prevent function creep and scope creep (as far as possible) in relation to the use of IDP identifiers, the TDIF should adopt measures to ensure that identifiers in the TDIF are not to be used for purposes outside the TDIF. In addition, measures should be implemented to ensure that consumers will always have a choice of more than one IdP in any TDIF transaction.
APP 10 – Quality of Personal Information	**Compliant**	The current TDIF concept and design include a range of measures to ensure data quality, but this initial PIA has not considered data quality issues in detail.	Some further work is being undertaken on related data quality issues, such as the time periods for validity and renewal of identities – noting that it is important that identity data is up to date having regard to the purpose of the use or disclosure.
APP 11 – Security	**Further action required**	The TDIF is being developed during a period of significant community concern regarding security and cybersecurity. Many agencies and organisations in Australia and elsewhere have been the subject of high profile attacks resulting in data breaches. APP 10 in the Privacy Act is only a small component of the broader security compliance framework that will apply to the TDIF. The key to complying with APP 10 is to implement security measures that are in proportion to the risk and impact of a breach of the data held in the TDIF.	Most of the security arrangements for the TDIF are not yet developed. Detailed security requirements have not been considered in this initial PIA.

Australian Privacy Principle (APP)	Status	Galexia Commentary	Recommendation
APP 12 – Access	**Further action required**	The TDIF Core Service Requirements should ensure that the Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transaction or identity fraud. In addition, each IdP will need to offer access to all the records that it holds on an individual, without restriction. In addition, some parts of APP 12 should be strengthened in the TDIF Core Service requirements in order to provide a consistent experience for consumers.	**R19: Access requests – Application in the TDIF** The TDIF Core Service Requirements should ensure that the Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transaction or identity fraud. In addition, each IdP will need to offer access to all the records that it holds on an individual, without restriction. **R20: Access requests – Consistency** In the Commonwealth Privacy Act the requirement that access will be provided within 30 days only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants (including the private sector) to ensure a consistent experience for consumers. Similarly, the 'free access' requirement only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants.
APP 13 – Correction	**Further action required**	Complaints and correction requests may cause some difficulties in the TDIF, as multiple participants may each hold part of the relevant data. The responsibility for complaints may be difficult to determine, and the complaints 'pathway' for consumers may be complex. Also, it is important for all TDIF participants to learn from complaints, so some sharing of complaints and complaints data across the TDIF will be useful. There is some inconsistency in the APPs in relation to complaints – different rules apply to agencies (government) and organisations (the private sector). In order to ensure a consistent experience for consumers, all TDIF participants should be required to meet the higher complaints standards.	**R21: Complaints coordination** It will be important to make the complaints and correction process 'clear and straightforward' for consumers. This may require TDIF participants to develop an appropriate referrals service. In addition, some data on complaints should be shared across the TDIF to ensure participants learn from complaints. **R22: Complaints – Consistency** In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints within 30 days.

1.4. Governance Arrangements

The DTA has recently commissioned an independent report on governance arrangements for the TDIF – "all options are on the table", and the DTA recognises the importance of governance in relation to privacy protection in the TDIF. The report will recommend governance models for the Federation (another consultancy relating to development of those rules will be issued once the options have been considered).

Although it is beyond the scope of this initial PIA to provide comprehensive advice on governance, some key high level principles on governance have emerged during the initial PIA, and these could be included in the DTA governance review.

R23: Governance arrangements

The DTA has recently commissioned a report on governance arrangements for the TDIF. The report should consider the following key governance issues (that have a direct impact on privacy protection):

A. Ensuring complete structural separation between the Identity Exchange and IdPs;
B. Ensuring an independent process is in place for TDIF accreditation;
C. Developing an appropriate underlying legal authority for the TDIF;
D. Developing appropriate coordination mechanisms for access and correction requests amongst TDIF participants, including the ability to share complaints data; and
E. Developing an appropriate mechanism for TDIF membership and ongoing engagement with stakeholders.

Further consideration of governance is set out in *Section 19. Governance*.

1.5. Recommended Future Privacy Work Plan

A suggested Future Work Plan for the DTA, based on the recommendations in this PIA, is set out at *Section 20. Recommended Future Privacy Work Plan* of this report. It utilises the following format:

Issue	Recommendation	Action Required	Person / Agency responsible	Method of Verification

2. Scope and Methodology

Galexia has conducted an initial Privacy Impact Assessment (PIA) for the Digital Transformation Agency (DTA) on the proposal to implement a Trusted Digital Identity Framework (TDIF) and related components.

2.1. Scope

The scope of this PIA is limited to the following items:

In Scope	Out of Scope
• High level identification of potential compliance issues in the context of the Australian privacy legal framework,	• Detailed compliance with specific sectoral / State or Territory legislation
• Review of *key* documents related to the TDIF, Identity Exchange and Commonwealth IdP proposals	• Review of the entire suite of DTA documentation
• Limited stakeholder consultation, including: - Internal staff members and suppliers (6) - Commonwealth OAIC - State and territory privacy regulators / officials (3) - State Agency Stakeholders (3) - Key privacy and consumer advocacy organisations (3)	• Extensive public consultation, open invitation consultation (there will be an opportunity for broader consultation in the Full PIA, scheduled for March 2017) • Consultation with every (or a broader cohort) of Commonwealth and State Agencies that may be touched by the TDIF.
• High level overview of security arrangements	• Full security audit
• High level identification and review of legal documentation	• Detailed legal advice

The DTA have agreed to conduct an independent and multi-phase PIA. This report is the initial PIA of the TDIF Alpha and the timing of this is prior to the development of a working prototype and before commencement of the beta phase – as defined in the DTA Digital Service Standard <https://www.dta.gov.au/standard/>.

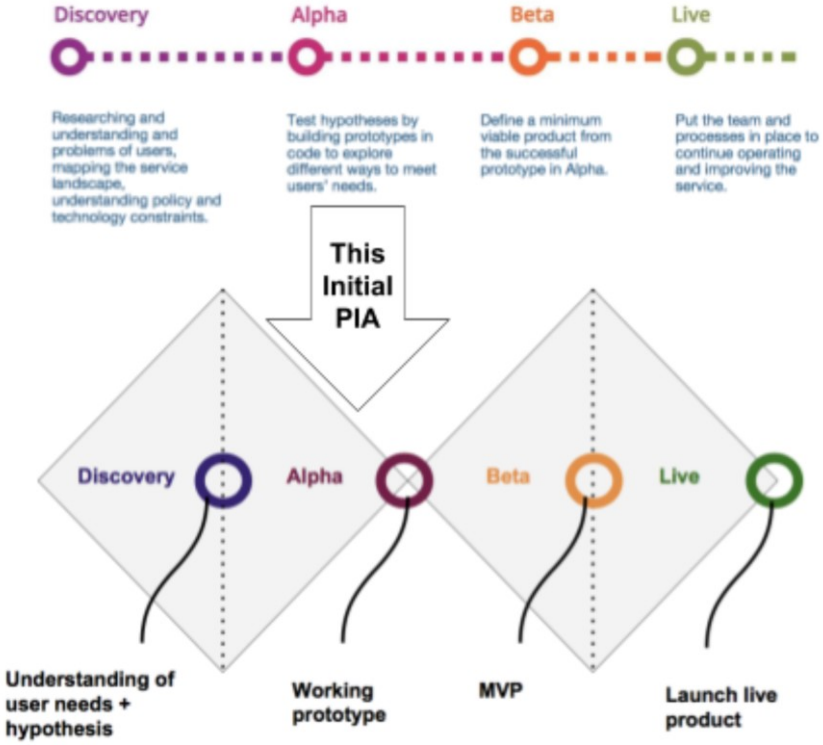


Diagram: Timing of this Initial PIA against the DTA Digital Service Standard

2.2. PIA Guidelines

This PIA is being conducted in accordance with the PIA Guidelines issued by the Office of the Information Commissioner.[2]

2.3. Privacy legislation

This PIA has been written in the light of current Commonwealth privacy legislation – the *Privacy Act 1988*. The Act sets out the Australian Privacy Principles (APPs),[3] which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations. The Act also includes a complaints, audit and enforcement regime.

In discussions with State and Territory stakeholders some issues and restrictions related to local legislation were raised. In this PIA, the focus is on compliance with Commonwealth legislation. However, the text includes brief references to local requirements where appropriate.

[2] <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide>

[3] The 13 APPs are in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*. They came into force on 12 March 2014

3. Trusted Digital Identity Framework (TDIF) Overview

3.1. Origins

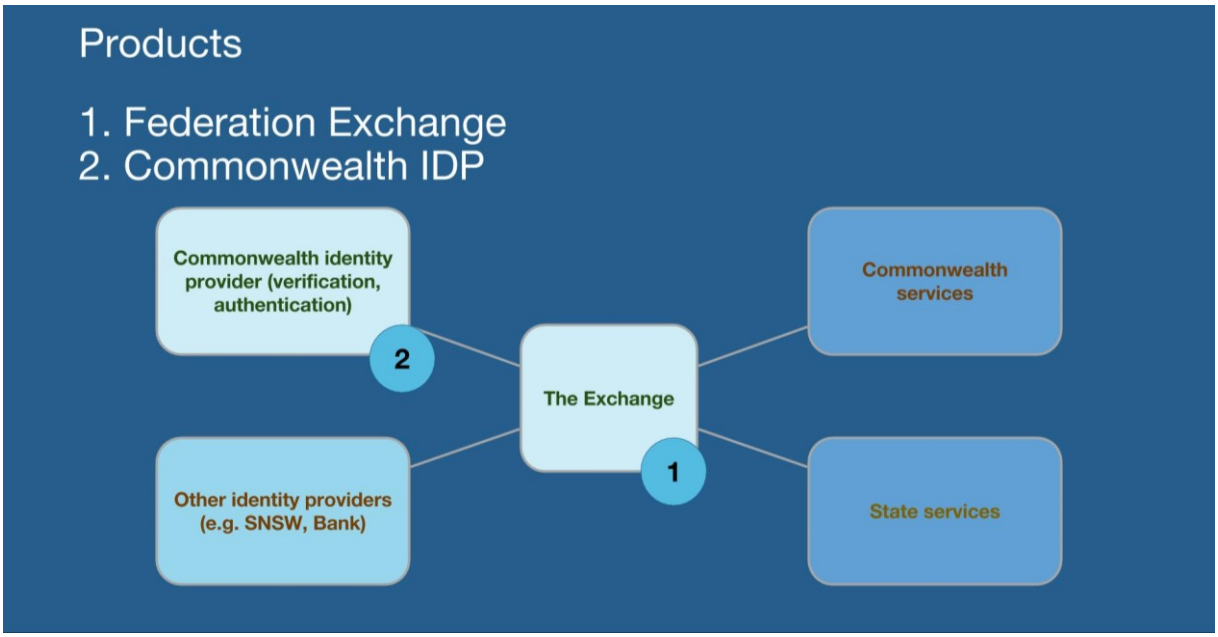
The Trusted Digital Identity Framework (TDIF) is a Commonwealth led initiative, overseen by the Digital Transformation Agency (DTA).The key components are:

1. The proposed development of mandatory standards, policies and agreements for all TDIF participants;
2. The proposed development of an Identity Exchange; and
3. The proposed development of a Commonwealth Identity Provider (IdP).

The key origin for the proposal is a recommendation by the Financial System Inquiry (The Murray report) in 2015:

> Inquiry Recommendation 15 — Digital identity
> Develop a national strategy for a federated-style model of trusted digital identities.[4]

The Commonwealth, State and Territory governments all have identity related initiatives in place. It is not the role of this PIA to provide an overview or history of the numerous initiatives, frameworks and standards that have been developed in this field. However, some of these historical initiatives do have an important impact on the 'context' of this PIA. For example, stakeholders are generally highly suspicious of any proposals in this field being an entry point to a more comprehensive / intrusive identity framework or products (such as earlier proposals for an Australia Card or an Access Card).



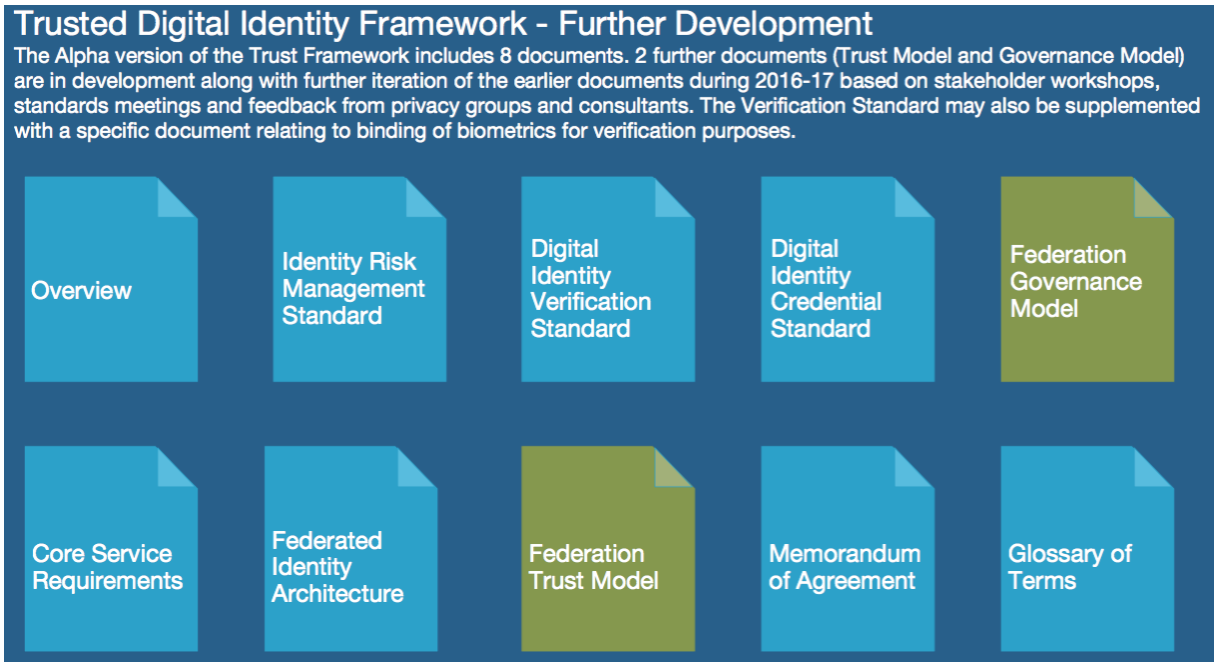
TDIF Overview of key components (Source: DTA, November 2016)

[4] Financial System Inquiry (The Murray Report), 2015, <http://fsi.gov.au/publications/final-report/>

3.2. Component 1: TDIF policies and standards

The first key component of the TDIF is the proposed development of mandatory standards, policies and agreements for all TDIF participants.

These documents are in the early stages of development – key document outlines have been distributed to stakeholders, but substantial work is required to develop the content of these documents.



TDIF Overview of key documents (Source: DTA, November 2016)

From a privacy perspective the key document is the *TDIF Core Service Requirements* document – this lists the privacy and security components that will apply to each TDIF participant.

Compliance with these standards will be mandatory – each TDIF participant will be accredited against the standards during their initial application to join the TDIF, and then on an ongoing basis. Reviews will be conducted on at least an annual basis.

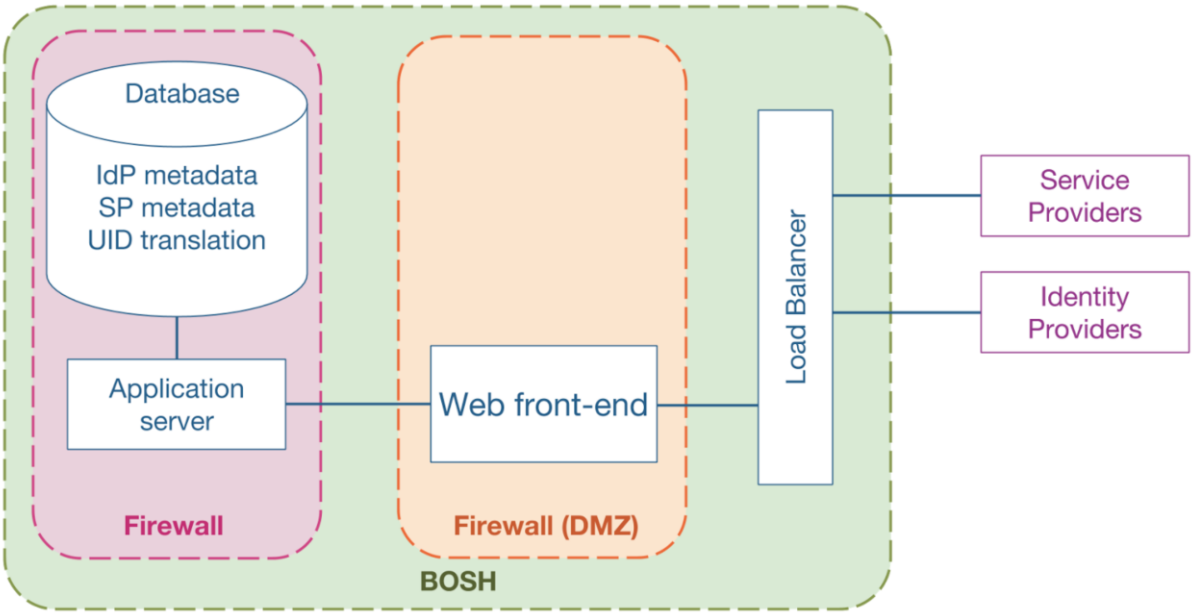
Refer to *Section 22. Appendix 2 – Background Information* for further detail.

3.3. Component 2: The Identity Exchange

An important component of the TDIF is the proposed Identity Exchange. This is a piece of infrastructure that is initially being built and run by the Digital Transformation Agency (it may be 'spun-off' as an independent entity at a future date). The Identity Exchange plays an intermediary role, as it sits between identity providers (IdPs) and Relying Parties.

The Identity Exchange plays a very limited and specific role in TDIF transactions. It enables identity assertions to be passed from any IdP to any Relying Party. It also allows a Relying Party to direct a new consumer to the Identity Exchange to either select an existing digital identity or enrol for a new one (from a list of IdPs). Consumers are presented with a list of digital identity options that can be used at that relying party (i.e. for that assurance level).

The Identity Exchange 'blinds' Relying Parties from IdPs and vice versa – this 'double blind' works by ensuring that the Relying Party receives an identity assurance that has been verified, without revealing the source of the assertion. Similarly, an Identity Provider cannot see the eventual Relying Party who relies on the identity assertion – they only know that a successful interaction at the appropriate level of assurance occurred via the Identity Exchange.



TDIF Identity Exchange high-level architecture (Source: DTA, November 2016)

This 'double blinding' is designed to be one of the privacy positive features of the TDIF. It means that the identity Exchange is not designed to become a central repository of identity data, and that IdPs do not obtain logs of the services being used by their customers. In addition, the Identity Exchange is able to provide consumers with a selection of IdPs, allowing personal data to be distributed across multiple providers rather than centralised in a single location.

However, some meta-data is retained by the Identity Exchange. This consists of the time stamp and basic connection details of each transaction. The metadata identifies the parties to each transaction, but does not include any other personal data that was provided during the transaction.

The meta-data held by the Identity Exchange is likely to be accessible in three ways:

- **By the consumer themselves** – for example the Identity Exchange can provide the consumer with a list of recent transactions. This access may be useful in assisting consumers to identify suspicious transactions;
- **By TDIF participants** – for example where a participant is investigating identity fraud or suspicious transactions or a suspicious pattern of transactions[5]; and
- **By law enforcement agencies, intelligence agencies and other third parties with appropriate legal authority** (such as a warrant or a subpoena). It is difficult to predict the full range of potential third party access, as there is a wide range of circumstances in which third parties can gain lawful access to data once it is collected.

[5] Note that the TDIF may also incorporate some automated processes that proactively monitor transactions looking for fraud and suspicious behaviour.

Although the overall design and objective of the Identity Exchange is to be privacy positive / privacy enhancing, the extent of protection provided by the Identity Exchange depends on several factors:

- The number of IdPs that a consumer can select for a TDIF transaction;
- The retention period for this meta-data; and
- The extent of third party access to the meta-data.

Many of these issue are not yet determined, and they are the subject of further discussion in this PIA.

3.4. Component 3: Identity Providers (IdPs)

IdPs play an important role in the TDIF. The entire model is built on multiple IdPs operating – the Murray Report (2015) recommended that multiple IdPs would foster competition and innovation in the provision of digital identities. Multiple IdPs also allow greater consumer choice, and can protect privacy as they avoid consolidation of large data sets and large trails of use.

At this early stage of development, the DTA is in discussions with several potential IdPs, including State and Territory governments and the private sector. The expectation is that the TDIF will begin operations with 'several' IdPs in place, Each IdP will be accredited against the standards described in Component 1 and use the Identity Exchange described in Component 2.

Some digital identity providers will continue to operate outside the TDIF – e.g. social identities (Google and Facebook) and lower level state and territory identities that chose not to join the TDIF.

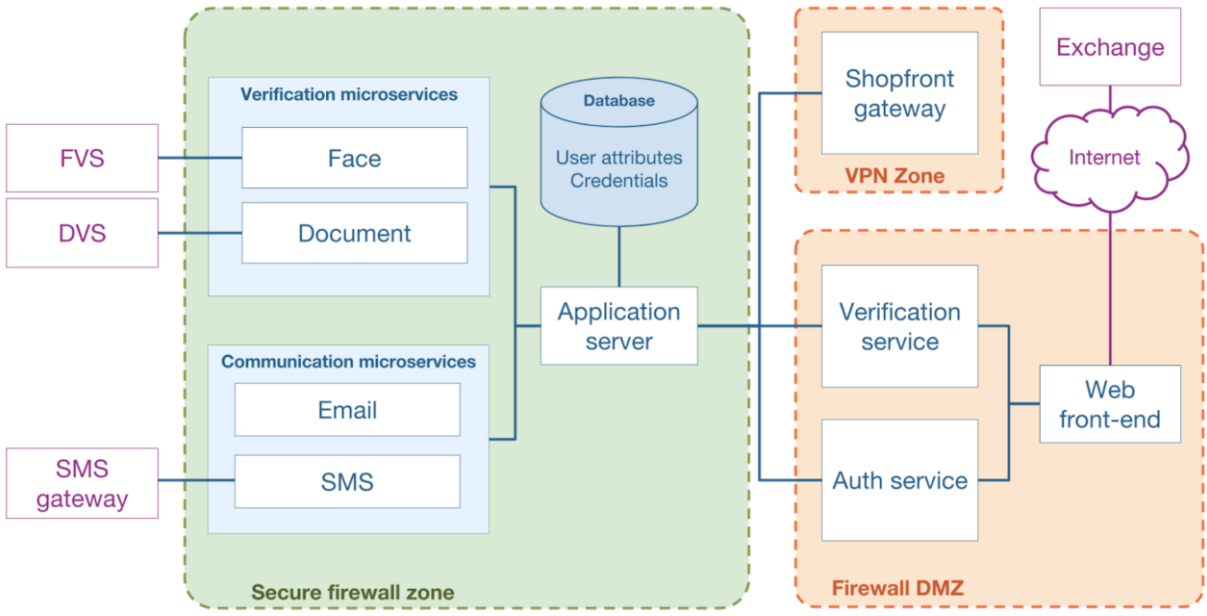
For the Commonwealth, a decision has been made to build and operate a single Commonwealth IdP. This would be the only IdP run by the Commonwealth, and would allow existing digital identities to be migrated across from services.

This is obviously a very significant decision at the Commonwealth level.

The proposed development of a single Commonwealth IdP is the subject of detailed discussion throughout this PIA. The following responses were presented by DTA as justification for a single Commonwealth IdP:

Justifications for several IdPs at the Commonwealth level	DTA justifications for a single IdP at the Commonwealth level
User Choice	• User research undertaken in the discovery phase revealed that consumers make little to no distinction between government agencies, even between Commonwealth and state agencies. It's all "government". • User research, and the experience of Verify.gov.uk, indicates that consumers find it difficult to know which provider they should choose when they are offered choice. Verify has conducted extensive iterative testing using multiple models for selection, with limited success in improving the process of selection. • Experience in federations where there are multiple IDPs, such as Verify in the UK, have shown that the user experience challenges are extremely difficult to overcome. Consumers face differing UI/UX challenges depending upon the provider. This has had severe impacts upon verification success rates. • User choice can be satisfied by providing state-level or private sector IdPs, e.g. banks. Research suggests that in this case choice is less likely to be about new providers and more about choosing a provider the consumer already has experience with, if it is available.

Justifications for several IdPs at the Commonwealth level	DTA justifications for a single IdP at the Commonwealth level
Competition between providers should lead to improvements in technology and service levels	• Commonwealth agencies do not effectively compete with one another. The goal of the APS is to be collaborative. In a federated identity model, there must be consistent standards across all providers. • This means that improvements to technology, security and user experience need to be effectively governed by the Federation, so that a relying party can have certainty about the levels of proofing and the processes and risks involved. This does not prohibit the introduction of new technologies but it means they must be done through the rules of the Federation, and this limits 'competition'.
Multiple Commonwealth IDPs would reduce the amount of records exposed if one of them was to suffer a breach.	• An effectively governed single IdP can focus efforts on security in one place instead of having to fund separate teams maintaining multiple instances • While a single IDP would certainly have some single security vulnerabilities, the reduction in numbers of people with administrative access to consumer data reduces the possibility for social engineering exploits on any data set.
Decentralisation of data across multiple Commonwealth IdPs could improve privacy protection by limiting linking of data via the Exchange	• Decentralisation of IDPs across multiple Commonwealth agencies offers no additional privacy protection, as agencies routinely share data via Memoranda of Understanding and the Data Sharing Act and will continue to do so.
Agencies are close to their customers and understand their needs with regard to identification and authentication.	• Agencies with service delivery obligations may feel the need to compromise standards for continuity of delivery. A verification and authorisation service that only does verification and authorisation has a reduced potential for compromise of standards. • Use cases and user needs can be very effectively dealt with through the Digital Service Standard. Moreover they can be done in manner that is truly whole of government as opposed to reflecting the needs of the service delivery agency.
–	• Reduction in number and cost of identity platforms



TDIF Commonwealth IdP high-level architecture (Source: DTA, November 2016)

3.5. Governance

The TDIF is a complex program involving multiple Commonwealth stakeholders, possibly all States and Territories, plus the private sector.

The TDIF is the subject of fairly minimal governance arrangement at this early stage of development. At this stage there is no:

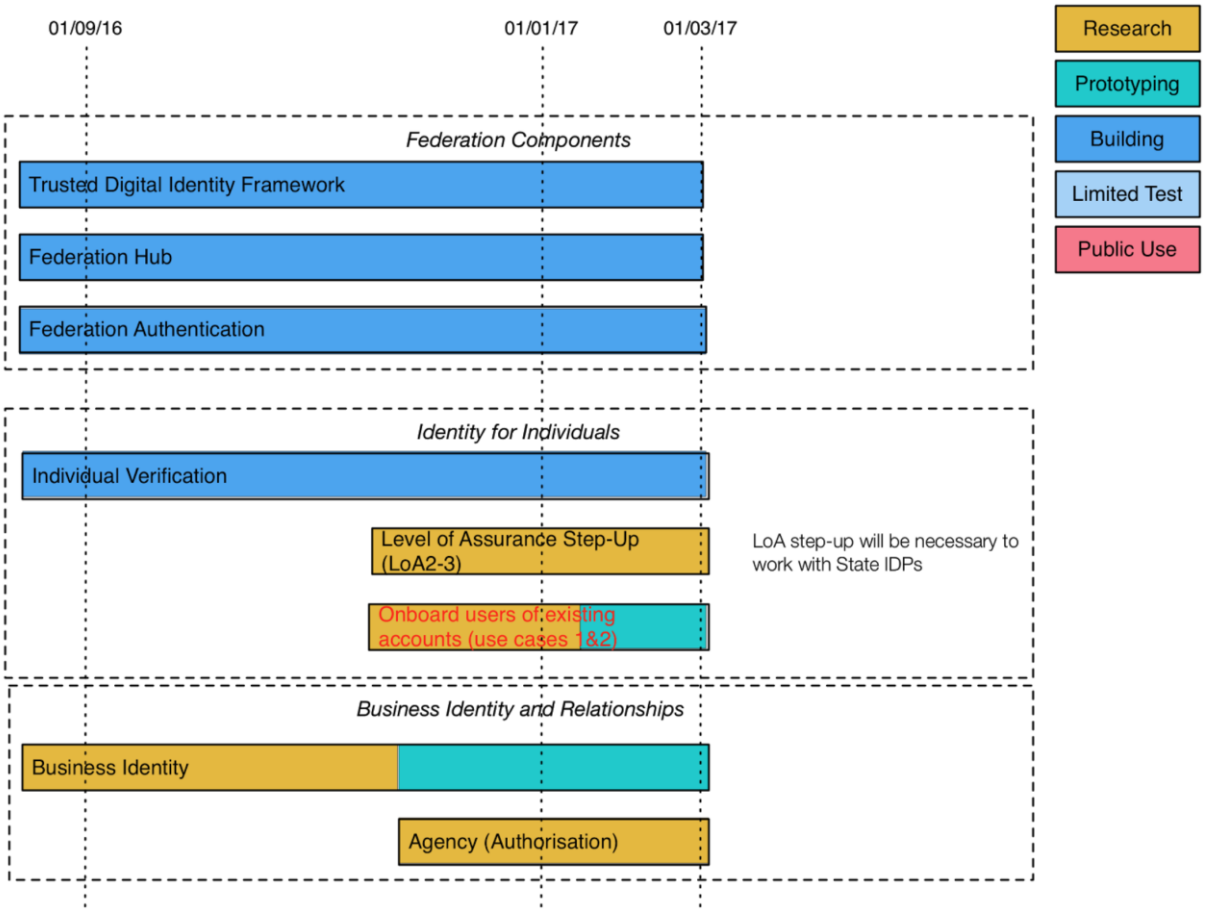
- Enabling legislation;
- Council of Australian Governments (COAG) agreement;
- Memoranda of Understanding between the parties; or
- Formal established board, working group or multi-jurisdictional committee.

However, there is an informal commitment to regular stakeholder consultation, and several large stakeholder meetings have already occurred, with more planned for 2017. A more formal governance structure will be developed shortly – the DTA has commissioned a report on Governance options, and this report is expected to be available by early 2017.

As the exact nature of governance is not yet determined, some suggestions are made on this issue later in the PIA.

3.6. Timeline

The following provisional timeline was provided by DTA with the understanding that it was a proposed schedule and subject to Government approval:



TDIF Provisional Timeline (Source: DTA, November 2016)

4. High level privacy issues for each TDIF component

Each of the TDIF components raises slightly different privacy issues. This PIA follows the Commonwealth PIA Guidelines, so each section examines compliance against a specific Australian Privacy Principle (APP). However, it is also useful to examine the *overall* privacy issues facing each TDIF component.

4.1. Component 1: The TDIF policies and standards

The first key component of the TDIF is the proposed development of mandatory standards, policies and agreements for all TDIF participants.

These documents are in the early stages of development – key document outlines have been distributed to stakeholders, but substantial work is required to develop the content of these documents.

As these policies and standards are mandatory, there is the potential that the TDIF will drive an improvement in the implementation of digital identity in Australia. TDIF participants will be evaluated against the standards at the time of application, and then on an ongoing basis (through a series of regular audits). They risk having their accreditation revoked if their processes and practices fail to meet the standards.

In turn, the standards include some sections on privacy and security (in the TDIF Core Service Requirements), although the details of these requirements are still in draft and require further development.

Overall, these arrangements would appear to be positive for the protection of privacy, and they received favourable comments from many stakeholders during the consultations for this initial PIA.

However, many commentators noted that:

- The standards are still being developed, and 'the devil is in the detail';
- Standards in similar previous frameworks were not enforced and were regularly breached without consequence (the example generally provided was the Gatekeeper PKI Framework, although analogies were sometimes made with similar schemes such as electronic health records);
- Stakeholders were extremely sceptical about the likelihood of the TDIF revoking the accreditation of a Commonwealth or State / Territory IdP – they believed that it would be very unlikely;
- Stakeholders were also extremely sceptical about the likelihood of the TDIF revoking the accreditation of a private sector IdP, particularly if that IdP was a major bank with (potentially) millions of customers; and
- Stakeholders were uniformly concerned about the potential impact of revocation of an accredited IdP on individual customers, who may face difficulties changing providers, especially in a small market.

Overall, the confidence expressed in the TDIF accreditation / revocation system by DTA is not yet reflected in the broader community of stakeholders, including potential TDIF members such as the States. Some stakeholders viewed the proposed accreditation / revocation as naive and predicted that 'it will never happen'.

It is possible that the low expectations of success for the TDIF accreditation / revocation proposal are linked to the absence of any legislative basis or national agreement (such as a COAG directive) for the TDIF. If stakeholders could see a firm commitment backed by powers in legislation, some of the doubts regarding enforcement may lessen.

Recommendation 1: The TDIF Membership Accreditation / Revocation Proposal

The development of the TDIF membership proposal, including accreditation and revocation, would benefit from significant further work on developing the detailed provisions and legal backing / powers / national agreement for the proposal, followed by further consultation with stakeholders. Stakeholders currently have very low expectations that this aspect of the TDIF can be developed or enforced.

A more specific privacy issue that arises in discussions regarding the mandatory standards and policies, is the question of which privacy principles should be incorporated into the TDIF Core Service Requirements.

This issue is not yet determined, but the DTA is developing a set of Core Service Requirements that utilise a customised set of Privacy Principles that reflect the highest possible standard available once all jurisdictions are taken into account. For example, starting with the APPs (which apply to the Commonwealth and the private sector), the Core Service Requirements could add or 'tweak' principles that appear in State and Territory privacy legislation until every possible requirement was covered by the new set of omnibus principles.

This approach would have the added advantage of setting standards for those jurisdictions where there are currently no legislated privacy principles in place (South Australia and Western Australia).

In (limited) consultations with stakeholders during this PIA it has become clear that there are mixed views on this approach:

- Some jurisdictions face challenges in allowing their covered agencies and organisations to adopt principles that are different from the principles in the local legislation;
- Some stakeholders were concerned that the proposal could create significant inconsistency within an organisation – where parts of the organisation complied with the APPs while other parts of the organisation had to comply with the TDIF Core Service Requirements. For example, a bank might end up with two different time limits for responding to access requests for the same customer - one period for general banking (under the APPs) and one period for digital identity (under the TDIF). The same issue would arise for some government agencies;
- The inconsistent principles were likely to cause problems and complexity for privacy regulators dealing with investigations, complaints and audits;
- The application of the principles in the Core Service Requirements might not meet current legislative tests for the transfer of data across borders, especially to jurisdictions where the principles would not be backed up by an independent privacy regulator;
- Even where the proposal was supported, stakeholders noted that privacy laws were very complex in Australia, and (again) the 'devil was in the detail'; and
- Stakeholders noted that if the TDIF was ever to be used in the health sector, additional specific principles apply in some jurisdictions in relation to personal health data (although the design of the TDIF precludes any actual health data being shared or disclosed, as the TDIF only plays a role in verification and authentication).

Stakeholders expect to be consulted further on this proposal, and to have an opportunity to review the proposed principles in the Core Service Requirements. There is also an expectation that the DTA will develop measures to address some of the practical concerns expressed above – all stakeholders are very wary of 'complexity' in the system.

Some stakeholders proposed alternative options, although these ideas also require significant further development:

- The TDIF could just adopt one existing set of principles (e.g. the APPs) and develop a mechanism for participants to 'opt-in' to coverage by those principles;
- The TDIF could recognise the federated nature of Australian privacy legislation, and apply slightly different standards to accreditation in each jurisdiction. In practice, this may have a knock-on impact on the design of the Identity Exchange, which currently 'blinds' parties from knowing where each identity is used;
- The TDIF could be used as a trigger or lever to seek a broader review of Australian privacy legislation to drive harmonisation and consistency; and / or
- The TDIF could be limited to those jurisdictions who already have strong privacy laws and independent regulators in place.

All of these suggested options face challenges of their own. Some of them introduce extra complexity or uncertainty and would require significant further discussion before they could be integrated into the TDIF drafts.

Overall, there was some limited support for the DTA's proposed development (and enforcement) of a new set of privacy principles to be incorporated in the Core Service Requirements, but stakeholders recognised that the proposal is in the very early stage of developments, and that further discussions and the broader circulation of a more fully developed set of draft principles may help to clarify the issue.

A further issue for consideration is the need to provide a consistent experience for consumers – this is one of the key objectives of the TDIF. The DTA review of international experiences in developing digital identity frameworks noted the difficulties caused by inconsistent user experiences (e.g. in the early implementation of verify.gov.uk), and the negative impact this had on enrolment rates. In this context it is important to note that the APPs themselves contain numerous areas of potential divergence: Even if all TDIF participants applied the APPs (or a slightly amended version of them), individual organisations could provide a completely different experience to consumers. Some examples include:

- **APP 6 Secondary use**
  Allowing each IdP to pursue its own secondary use could be a very dangerous approach in the TDIF – the limits on secondary use should be set out in the TDIF Core Service Requirements and applied consistently to all participants;
- **APP 7 Direct marketing**
  APP 7 allows direct marketing, but this is likely to be completely outside the expectations of TDIF customers. Direct marketing in the TDIF should be prohibited without exception, to ensure consistency between government and private sector IdPs. This will also help to address concerns about private sector profiling of individuals in the TDIF;
- **APP 8 Cross border data transfers**
  APP 8 allows organisations to select from three completely different compliance approaches – direct responsibility, adequacy and consent. This approach could lead to completely different experiences for consumers across the TDIF;
- **APP 12 Access requests**
  Different standards for access requests apply to agencies (Government) and organisations (the private sector) – for example the requirement for replies to be issued within 30 days and the provision of free access only apply to agencies under APP 12; and
- **APP 13 Complaints and corrections**
  Different standards for corrections apply to agencies and organisations – for example, only agencies are required to respond to complaints within 30 days. It will be important to remove those distinctions in the TDIF.

In addition to the opportunity to select the strongest option for privacy protection from each jurisdiction, the TDIF Core Service Requirements present an opportunity to select the strongest privacy protection within the options available in the APPs. If this approach is not taken, the APPs will allow significant discretion and divergence.

This approach does represent a small additional burden for some TDIF participants (e.g. private sector IdPs who would be subject to lower standards if they only applied the APPs), but it appears to be an appropriate trade-off for the benefits of TDIF accreditation.

Recommendation 2: Privacy Principles in the Core Service Requirements

The DTA should consider the full range of options for incorporating privacy principles in the TDIF Core Service Requirements. The strengths and limitations of each option should be considered side-by-side, and discussed with key stakeholders. This discussion would benefit from the development of draft principles that attempt to set the highest possible standard based on existing laws in each jurisdiction, but this option should not be the only option available for discussion. Practical issues for the implementation of each option should also be considered, and solutions proposed.

4.2. Component 2: The Identity Exchange

The Identity Exchange includes elements that are designed to minimise the amount of personal data that is collected and stored, to 'blind' IdPs and relying parties from information about the detailed use of identities, and to provide consumers with choice about which identity they use in each transaction.

All of these elements were clearly recognised by stakeholders as being privacy positive. During the consultations conducted in this PIA, the following views were expressed:

- Stakeholders generally described the Identity Exchange as the most privacy friendly component of the TDIF;
- Stakeholders recognised that the Identity Exchange reduced some of the privacy impact of 'logs' that were required in other identity schemes (notably PKI schemes);
- Stakeholders predicted that some consumers would be attracted to the choice that was enabled by the Identity Exchange; and
- Stakeholders noted that the Identity Exchange helped minimise the overall collection and sharing of personal data, and that data minimisation is a key privacy protection measure.

However, stakeholders did express two common concerns regarding the Identity Exchange and privacy.

One of the concerns relates to the relevance (from a privacy protection perspective) of the Identity Exchange in a scenario where there are only one or two IdPs. This issue is discussed in more detail in the section on IdPs below.

The second concern is related to the collection, use and disclosure of metadata by the Identity Exchange. The most common stakeholder views included:

- Although the meta-data did not include the full personal details of each transaction, it was still a very rich source of personal data;
- Broad access to the meta-data would enable surveillance (of individuals or large parts of the population) in an environment where consumers had very little protection against surveillance. Stakeholders believed that privacy regulators were weak in the face of surveillance requests, intelligence agencies are often exempt from privacy laws, Australia has no Bill of Rights and Australia has no private right of action for serious privacy intrusions;
- Access to the meta-data was likely to be expanded in the future (function creep or scope creep);
- Access to the meta-data can be easily combined with access to IdP and relying party records to gain a complete picture of an individual's transactions;
- The meta-data might be the subject of a hack or breach and exposed – it represented an attractive target for external attack; and
- Although the Identity Exchange currently only retains meta-data, it could easily be expanded in the future to retain additional personal data (function creep or scope creep).

Many of these concerns were expressed in the broader context of the lack of specific legislation for the TDIF or other sources of legal authority. However, stakeholders were careful to stress that privacy concerns could not necessarily be 'cured' by legislative backing. Some stakeholders had very low expectations that legislation could restrict use of the meta-data appropriately in the current political environment, which they saw as strongly favouring surveillance over privacy rights.

In consultations with stakeholders we explored potential mechanisms to mediate concerns about the metadata collected by the Identity Exchange. The potential measure of most interest was the development of a very short retention period for the meta-data. This would help to minimise the amount of data stored, therefore reducing the attractiveness of the data as a target for surveillance or external attack, and reducing the impact of any disclosure or breach. Stakeholders did not have firm or consistent views on an appropriate period for data retention – suggestions ranged from a few minutes to 12 months.

In discussions with DTA senior management, it was suggested that a major driver for retaining the meta-data is to facilitate the investigation of identity fraud and suspicious transactions. DTA agree that further research on how long meta-data needs to be retained for the purpose of investigating identity fraud might help to determine an appropriate data retention period. The period suggested by such research would need to be weighed against the additional privacy risks and impacts of retaining the data.

Recommendation 3: The Identity Exchange and the retention of metadata

DTA should conduct further research on the period that meta-data needs to be retained in order to facilitate the investigation of identity fraud and suspicious transactions. This period should then be 'balanced' against the privacy risks and impacts of retaining the data, and an appropriate data retention period should be incorporated into the design of the Identity Exchange. For the avoidance of doubt, an 'appropriate period' could be shorter than the period required for all investigative purposes.

4.3. Component 3: Identity Providers (IdPs)

IdPs play an important role in the TDIF. The entire model is built on multiple IdPs operating, with stakeholder expectation that there will be IdPs at the Commonwealth level, at least some State and Territory IdPs and potentially some private sector IdPs.

At the Commonwealth level, the DTA has decided to develop a single IdP. Existing Commonwealth digital identities will be transitioned to the Commonwealth IdP, and no further IdPs will be allowed to develop at the Commonwealth level.

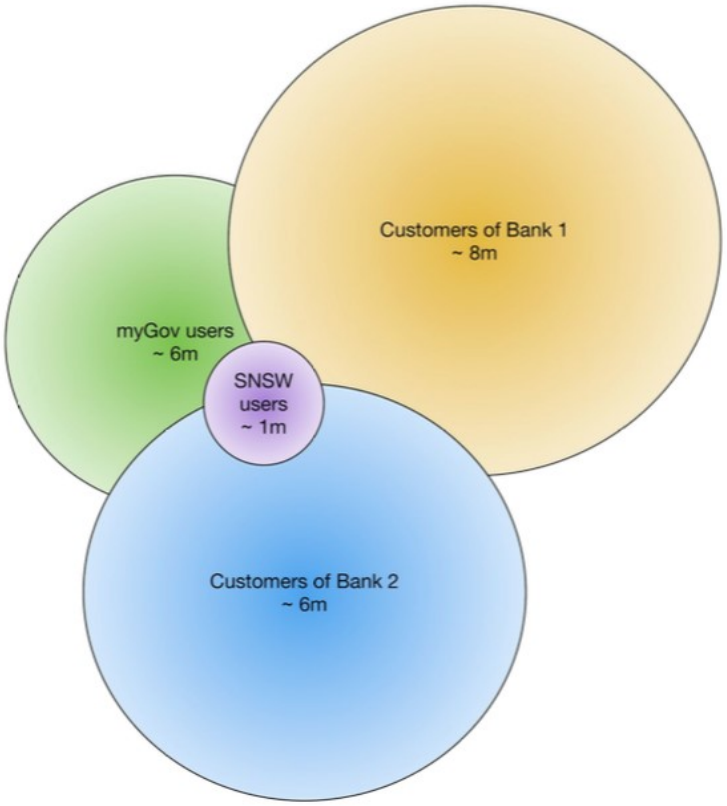
In contrast to the Identity Exchange, IdPs do collect and store significant amounts of personal data.

The proposals relating to IdPs are the subject of significant privacy concerns from stakeholders, and these are discussed in detail below. A preliminary issue, raised by many stakeholders, is the sense that the decision to develop a single Commonwealth IdP has not been justified or explained by the DTA.

In the consultation conducted for this PIA, the following views were expressed on this issue:

- Stakeholders questioned where the decision had 'come from' as it appeared to take nearly all stakeholders by surprise;
- Stakeholders queried the link between the decision to establish a single Commonwealth IdP and the recommendations of the Murray Report (which in part endorses the development of multiple IdPs in order to foster competition, choice and innovation);
- Stakeholders queried whether due consideration had been given to the failure of previous centralised models in the Commonwealth identity field, such as the Australia Card and the Access Card. Although stakeholders recognised some differences between those proposals and the TDIF in relation to the overall framework and the Identity Exchange, they viewed the decision to establish a single Commonwealth IdP as a 'throwback' to those earlier proposals. Even after detailed discussions and explanation on the details of the TDIF most stakeholders still viewed the single Commonwealth IdP as an updated version of the Australia Card / Access Card;
- Stakeholders were strongly of the view that such an important and far-reaching decision should have been the subject of extensive community consultation and debate, with many stakeholders calling for a public discussion paper and / or legislation; and
- Almost all stakeholders struggled to see any justification for the establishment of a single IdP – a common question was "what is the problem that needs to be solved?"

The DTA has provided a series of key counter arguments. It is their view that there will be multiple IdPs, and that consumers will have choice, and that the Commonwealth IdP will not even be the largest IdP. However, when these counter-arguments were raised with stakeholders they were dismissed as an insufficient response to the seriousness of the issues, or viewed as 'unlikely' scenarios or unachievable solutions in practice. Stakeholders had low expectations that multiple IdPs would be available, and they expected the Commonwealth IdP to be a large and significant entity. Many stakeholders expressed the view that the Commonwealth IdP would be almost the 'default' provider for many consumers.



TDIF Candidate IdPs (Source: DTA, November 2016)

One important challenge raised by the juxtaposition of the Identity Exchange and the single Commonwealth IdP is that in discussions regarding the two components, privacy strengths in one component highlight privacy weaknesses in the other component.

Some examples include:

- A *strength* of the Identity Exchange is that it minimises the amount of personal data collected and stored. The significant amount of data stored and collected by the IdP is then viewed as a weakness.
- A *strength* of the Identity Exchange is that it does not ask for any biometric information. The requirement to provide biometric information to an IdP (during enrolment) is then viewed as a weakness.
- A *strength* of the IdP model is that there are numerous IdPs and consumers have a choice about which one to use, therefore minimising centralisation of data. This is then viewed as a weakness of the Identity Exchange as there is only one Exchange, and meta-data is centralised in one entity.

Finally, stakeholders queried whether the single Commonwealth IdP model 'stacked up' against other options. Each stakeholder had their own view on alternative models, but the range of options included:

- A 'fully' distributed model, such as a peer-to-peer network of IdPs;
- Allowing all Commonwealth IdPs to become TDIF accredited if they wished;
- Having a mix of several large Commonwealth IdPs and then a single IdP for smaller agencies
- A personally controlled identity product; and / or
- A store of attributes, rather than identities.

It is not the role of this PIA to flesh out these alternative options in more detail, but stakeholders were concerned that alternative options had not been considered (either at all or in sufficient detail).

Overall, stakeholders were highly critical of both the decision to establish a single Commonwealth IdP and the process (or perceived lack of process) in making that decision.

In subsequent discussions with the DTA it is clear that the decision has been iterated over some time on the basis of internal discussions and meetings with the current providers of Commonwealth identity services (for example MyGov, the Australian Taxation Office and the Department of Human Services), and that some research and testing with consumers had been undertaken on the issues and perceptions regarding IdPs. Further, to assist with this PIA, the DTA prepared a detailed written explanation of the benefits of the single Commonwealth IdP model (extracted in Section 3.4 of this report).

Also, the DTA do not accept that the single Commonwealth IdP model is a departure from the recommendations of the Murray Report, as the entire purpose of the TDIF is to build a community of multiple IdPs.

Nevertheless, it is difficult to point to a written analysis and justification for the single Commonwealth IdP model that is available to stakeholders. The decision is significant, and it is natural that the approach to IdPs at the Commonwealth level should be the source of major stakeholder concern (considering the long history of centralised identity proposals by the Commonwealth).

This may therefore be an appropriate time to pause the development of the single Commonwealth IdP and take steps to ensure that the proposal has the required level of stakeholder and community understanding and support. This could take the form of a specific workshop (or series of workshops) on this aspect of the TDIF, or the development of a discussion paper, followed by broad consultation and review, or both.

Recommendation 4: The selection of a single Commonwealth IdP – Further consultation

The DTA should recognise stakeholder concerns regarding the decision to establish a single Commonwealth IdP and should take steps to ensure that the proposal has an appropriate level of stakeholder and community understanding and support before implementing the proposal.

The proposal to establish a single Commonwealth IdP also raises potential risks for the overall TDIF, and it is unclear whether these risks have been the subject of appropriate discussion and review. Certainly stakeholders believed that these issues had not been discussed with them. Potential risks include:

- **The potential for reducing the number of available IdPs**, therefore limiting consumer choice and undermining some of the objectives of the TDIF in relation to privacy protection, competition and innovation;
- **The potential for consolidating a large amount of personal data in a single database**, therefore potentially raising the risk profile of that data (as the larger data set is more attractive to external attack) and also potentially raising the impact on the community if there is a breach of that particular data set; and
- **The potential for simplifying and streamlining access to a large amount of personal data**, therefore potentially establishing a platform for future surveillance by Government or access by third parties (function creep and scope creep).

Although the DTA may have considered some or all of these issues in its development of the proposal, the TDIF would benefit from a comprehensive risk review of the single Commonwealth IdP model, that examines the likelihood of these risks occurring and the potential severity of their impact if they did occur (in comparison to the risks of other options). The risk review could also consider potential risk mitigation measures.

Recommendation 5: The selection of a single Commonwealth IdP – Risk Assessment

The DTA should commission an independent risk assessment of the proposal to establish a single Commonwealth IdP, in comparison to the risks of other options, to ensure that the consequences of the proposed model do not represent an unacceptable risk to the community.

In addition to the *broad* concerns regarding the establishment of a single Commonwealth IdP, stakeholders expressed a number of specific privacy concerns. Many of these concerns also apply to other IdPs (e.g. State and Territory IdPs and private sector IdPs).

During the (limited) consultations for this PIA a long list of privacy issues in relation to IdPs was raised by stakeholders.

Some of the key views include:

- Each IdP will develop an identity number, and stakeholders were concerned about the potential use (and reuse) of that number. Even if there is no intention to use that number now, stakeholders were concerned about future applications (function creep and scope creep);
- Each IdP will obtain, over time, a large and rich source of personal data that will be attractive to third parties for surveillance, and / or subject to external attack (e.g. hackers), and / or subject to accidental breach. The consequences of surveillance or a breach were likely to be significant. This was often raised as a very strong argument against the consolidation of Commonwealth identity provision into a single Commonwealth IdP;
- Some stakeholders predicted that, over time, each IdP would collect biometric information (photographs) and contribute to the development of a national data set of photographs. Although there is no intention to retain photographs in the TDIF, and they are destroyed as soon as a verified match has been made, stakeholders believed that 'it was only a matter of time' before the system was changed and photographs were retained and shared; and
- Some of the data collected and retained by IdPs was not actually necessary for many online transactions, but would be collected by default as part of the TDIF. The two security levels (Level 2 and Level 3) were seen by some stakeholders (particularly State stakeholders) as arbitrary levels imposed by the Commonwealth without reference to the needs of actual applications. Many stakeholders expressed the view that identity requirements were constantly 'ratcheting up' with little regard to the actual transaction risks involved. Identity requirements never lowered. It was noted that the Identity Exchange effectively 'blinded' parties to the use of identities, and this may have the unintended consequence of further ratcheting up' identity requirements.

5. Is the data 'personal information'?

5.1. The Law

A starting point for our discussion of privacy compliance is whether or not the data collected in the TDIF is personal information.

The Commonwealth Privacy Act states:

> Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.
> <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#personal-information>

The Office of the Australian Information Commissioner has provided some further guidance on whether an individual is 'reasonably identifiable':

> Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:
>
> 1. the nature and amount of information
> 2. the circumstances of its receipt
> 3. who will have access to the information
> 4. other information either held by or available to the APP entity that holds the information
> 5. whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'
> 6. if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

However, these guidelines are not binding, and the definition of personal information is the subject of ongoing debate. The definition is currently the subject of an Appeal[6] by the Privacy Commissioner from a decision by the Administrative Appeals Tribunal (AAT), so some binding guidance on the definition may become available later in 2016. The AAT decision concentrates on whether or not information is 'about an individual', and broadly concludes that even though data might identify someone, it is not 'personal data' if it wasn't about the individual (e.g. where the individual's identity is revealed by accident).

The Guidelines conclude with the following warning:

> Where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information.

[6] The Commissioner is appealing the decision in Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 which overturned a previous determination by the Privacy Commissioner in Ben Grubb and Telstra Corporation Limited [2015] AICmr 35.

5.2. TDIF – Overview

The Trusted Digital Identity Framework (TDIF) incorporates a mix of personal information, metadata and non-personal information.

The key store of personal information is the data collected and held by the IdPs at the time of enrolment. I

The current TDIF design envisages the following data will be collected during enrolment. It is important to note that this table refers only to data collected and stored by IdPs – the collection of data by the Identity Exchange is discussed later in this section.

The table below indicates that the IdPs collect and hold considerable personal data.

Data element	Is it personal information?	Collection	Use	Storage
Full name	**Yes**	Collected at enrolment	Verification and authentication	Stored permanently by the IdP
Date of birth	**Yes**	Collected at enrolment	Verification and authentication	Stored permanently by the IdP
Address	**Yes**	Collected at enrolment	Address data is not verified, but the 'asserted' address is an attribute that can be shared under the TDIF with the customer's consent.	Stored permanently by the IdP
Email address	**Yes**	Collected at enrolment	Used for sending security tokens and password resets.	Stored permanently by the IdP
Mobile phone number	**Yes**	Collected at enrolment	Used for sending security tokens.	Stored permanently by the IdP
Face image / photograph / biometric template	**Yes**	Collected at enrolment (exact process under development)	Used only for verification at enrolment	Checked against the Face Verification Service (one time only). Image / photograph / biometric template then deleted. Some form of transaction record / receipt maintained to provide assurance that the match was undertaken.
Evidence of Identity Documents. (The exact number and nature of the documents depends on the individual, but sufficient to comply with the standards for each level of identity.)	**Yes**	Collected at enrolment. ● For online enrolment the consumer will be asked for a photograph of each document. ● For face to face enrolment the documents can be presented.	Used only for verification at enrolment	Checked against the Document Verification Service (one time only). Photographs of documents are then deleted. Some form of transaction record / receipt maintained to provide assurance that the match was undertaken.

There will be a few brief periods where data is in transit (such as the Yes / No response from the FVS or DVS) where that specific data element will not contain personal information, and although it is encrypted in transit it is theoretically possible it could be linked (via the Verification Request Receipt Number and / or the timestamp of the transaction if these were decrypted by an actor with sufficient resources / legal authority) to other data that would identify the individual. For the IdPs *all* of this data should be treated as personal information for the purposes of the Privacy Act.

Each IdP is also likely to apply a unique identifier / number to each record in its database to ensure the uniqueness of each record (such as a Globally Unique Identifier or GUID). Individuals can only have one digital identity in their personal capacity in each IdP[7]. (They may also have a separate digital identity in their business capacity in each IdP). There is no requirement or need for this unique identifier / number to be used in the day-to-day activities of the TDIF, but it will exist. This unique identifier / number should be treated as personal data for the purpose of the Privacy Act as it is clearly linked to data that would identify the individual.

The Identity Exchange will also collect, use and store some personal data, although the majority of data that it processes will be simply 'passed through' and not retained.

In the TDIF project the data retained by the Identity Exchange is referred to as meta-data as it is limited to the identities of the parties and the timestamp of the transaction – the content of the transaction and any communications content is not retained. However, use of the term meta-data in this context does NOT mean that the data is not personal information for the purposes of the Privacy Act. Indeed, the content of the metadata is a rich source of personal data and is linked directly to the identity of the individual (the Identity Exchange uses different identifiers, but these are translated from identifiers provided by the IdP and these can be re-linked with the cooperation of both parties). The meta-data reveals the type and frequency of services that the individual is contacting, although it does not reveal the content of those contacts. The meta-data also reveals the number and identity of the IdPs that are utilised by consumers, although it does not reveal the detailed information held about individuals by those IdPs. For the purposes of the TDIF, the meta-data held by the Identity Exchange should always be treated as personal information in relation to compliance with the Privacy Act.

5.3. 'Personal information' finding

The Privacy Commissioner warns that "where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information".

In the case of the TDIF this PIA concludes that all data collected, stored and used by Identity Providers (IdPs) should be classified and treated as Personal Information under the Privacy Act.

The States and Territories are subject to slightly different interpretations of the term 'personal information' but this is a good example of a situation where the TDIF Core Service Requirements can be used to achieve some consistency across jurisdictions. The Core Service Requirements should insist that all IdPs classify and treat their data as personal information and protect all of this data in accordance with the privacy provisions set out in the remainder of the Core Service Requirements (currently under development). This will remove opportunities for IdPs to seek technical or definitional reasons to avoid applying privacy protections to some types of data under their control, and will improve confidence for users that their data is subject to strong privacy protections.

Recommendation 6: Identity Providers and the definition of Personal Information

All data collected, stored and used by Identity Providers (IdPs) should be classified and treated as Personal Information.

[7] There may be some very limited circumstances where an individual has more than one identity in an IdP.

This PIA also concludes that all data collected, stored and used by the Identity Exchange should be classified and treated as Personal Information under the Privacy Act.

Recommendation 7: The Identity Exchange and the definition of Personal Information

All data collected, stored and used by the Identity Exchange should be classified and treated as Personal Information.

6. APP 1. Open and transparent management of personal information

6.1. The Law

APP 1 — open and transparent management of personal information

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the APPs / registered code; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs / registered code.

1.3 An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 (minimum contents of the privacy policy)

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

6.2. TDIF – Overview

The TDIF is at an early stage of development, and this initial PIA is limited to a high level review of the concept and design of the TDIF and its core components. At this early stage it is difficult to provide detailed advice on compliance with APP 1, but we can point to some key privacy issues that will be relevant to the TDIF.

The likely approach in the TDIF is that participants will be bound by the APPs or similar principles at least as strong as the APPs, either through specific TDIF legislation or through the TDIF Core Service Requirements. The exact governance arrangements are still under discussion. This level of protection will be strengthened by regular mandatory compliance audits.

APP 1 (or its TDIF equivalent) will apply to all TDIF participants (IdPs, Relying Parties and the Identity Exchange).

The following checklist provides a useful summary of the key issues regarding openness and transparency – these issues will need to be addressed in further detail in the full PIA (2017).

APP1. Openness and transparency	Action / Status	Galexia Commentary
A. Does the entity provide a public privacy policy?	**Current design is compliant**	IdPs will be required to develop a stand-alone privacy policy and submit it as part of their TDIF application. Relying Parties will need to amend or expand their existing privacy policies to incorporate references to key data collection, use and disclosure that is facilitated by the TDIF. The Identity Exchange will need to develop a stand-alone privacy policy.
B. Does the Policy include: (a) the kinds of personal information that the entity collects and holds;	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.

APP1. Openness and transparency	Action / Status	Galexia Commentary
C. Does the Policy include: (b) how the entity collects and holds personal information;	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.
D. Does the Policy include: (c) the purposes for which the entity collects, holds, uses and discloses personal information;	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.
E. Does the Policy include: (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.
F. Does the Policy include: (e) how an individual may complain about a breach of the APPs / registered code, and how the entity will deal with such a complaint;	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.
G. Does the Policy include: (f) whether the entity is likely to disclose personal information to overseas recipients;	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.
I. Does the Policy include: (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.	**To be addressed in the full PIA (2017)**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement.

6.3. APP 1. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

APP 1 (or its TDIF equivalent) will apply to all TDIF participants. Compliance should not present any difficulties, and participants will need to develop or amend their public privacy principles to explain the operation of the TDIF and its impact.

Recommendation 8: Openness task

Specific requirements on openness and transparency should be set out in the TDIF Core Service Requirements.

- IdPs will be required to develop a stand-alone privacy policy and submit it as part of their TDIF application.
- Relying Parties will need to amend or expand their existing privacy policies to incorporate references to key data collection, use and disclosure that is facilitated by the TDIF.
- The Identity Exchange will need to develop a stand-alone privacy policy.

7. APP 2. Anonymity and Pseudonymity

7.1. The Law

APP 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-2-app-2-anonymity-and-pseudonymity>.

7.2. TDIF – Overview

The TDIF is an identity framework designed to cater for transactions that require Level 2 and Level 3 identity. There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level.

7.3. APP 2. Finding

While not limiting or downplaying the requirement for agencies to provide anonymous and pseudonymous options to consumers in appropriate transactions and services on a case-by-case basis, APP 2 is not relevant to the TDIF, and is not the subject of detailed consideration in this PIA.

8. APP 3. Collection of solicited personal information

8.1. The Law

APP 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 [*list of exceptions, none of which are particularly relevant to collection in the TDIF*]

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Sensitive information[8] means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual orientation or practices; or
(ix) criminal record;
that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

8.2. OAIC Guidelines

The *PIA Guidelines* issued by the OAIC contain a set of hints and risks under the category of personal information to be collected.

The Privacy Risks they have identified include:

- Collecting unnecessary or irrelevant personal information, or intrusive collection; and
- Bulk collection of personal information, some of which is unnecessary or irrelevant.

In addition to these risks, the collection of personal information should generally be kept to a minimum and personal information should normally be collected from the data subject.

The *PIA Guidelines* also contain a set of hints and risks under the category of method of collection.

The Privacy Risks they have identified include:

- Individuals unaware of the collection or its purpose; and
- Covert collection is generally highly privacy invasive, and should only occur under prescribed circumstances.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

8.3. TDIF – Overview

The focus of information collection in the TDIF is the enrolment processes undertaken by the IdPs. Some of this data is later shared, with consent, with other TDIF participants.

The TDIF is at an early stage of development, and this initial PIA is limited to a high level review of the concept and design of the TDIF and its core components.

[8] Section 6 of the Privacy Act (1988) <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html>

At this early stage it is difficult to provide detailed advice on compliance with APP 3, but we can point to some key privacy issues that will be relevant to the TDIF.

The likely approach in the TDIF is that participants will be bound by the APPs or similar principles at least as strong as the APPs, through the TDIF Core Service Requirements. This level of protection will be strengthened by regular mandatory compliance audits.

APP3. Collection of solicited information	Action / Status	Galexia Commentary
A. Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	**Current design is compliant**	Each IdP will collect enough personal information to verify the identity of individuals. This will vary slightly for each consumer, depending on the EOI documents that they have available, and the level of identity they are applying for. The extent to which this information is "reasonably necessary" is set by the requirements for each identity Level. Some stakeholders have concerns that the levels are arbitrary and they are set at a higher level than needed. Some additional personal information is collected to ensure that more innovative security measures can be utilised. For example, email addresses and mobile phone numbers are collected so that IdPs can send one-time security tokens to consumers. Overall, APP 3 sets a fairly easy test for compliance, and the proposed data fields are likely to easily meet the test of 'reasonably necessary'.
B. Is NO sensitive information about an individual collected (unless a relevant exception applies, such as the receipt or explicit and specific consent)?	**Requires further review / action**	IdPs will collect some sensitive information in the TDIF, because the definition of sensitive information includes: (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates. As a result, IdPs will need to obtain specific explicit consent for the collection of this biometric information. During this high level initial PIA we have reviewed the demonstration prototype, which does seek general consent prior to the collection of personal data. The next iteration of the design will need to incorporate a request for specific explicit consent to the collection of biometric data. The project might benefit from some user testing regarding whether users understand the consent that they are providing in relation to the collection of biometric data.
C. Is personal information collected only by lawful and fair means?	**Current design is compliant**	No concerns have been identified or expressed regarding the means of collection.
D. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	**Current design is compliant**	All data is collected directly from the consumer. Some data is verified against other sources (the DVS and the FVS) with the clear consent of the individual.

8.4. APP3. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

Those principles should include a collection principle and sub-principles (that ensure collection is necessary, that collection only occurs by lawful and fair means, and that collection is from the individual concerned).

One item related to collection that requires further review is the collection of sensitive information. In the APPs this requires specific and explicit consent. In the TDIF this may be relevant because IdPs will be collecting biometric information during enrolment. In the demonstration prototype users are asked to submit a photograph of their face – a biometric 'template' is created based on this photograph and then checked against the Face Verification Service (FVS). Although the photograph is not retained, this process should be considered a collection of biometric data.

Recommendation 9: Collection of sensitive data

The next iteration of the TDIF design will need to incorporate a request for specific explicit consent from users to the collection of biometric data. This occurs at the enrolment stage. The project would benefit from some user testing regarding whether users understand the consent that they are providing in relation to the collection of biometric data.

9. APP 4. Dealing with unsolicited personal information

9.1. The Law

APP 4 requires organisations who receive unsolicited personal information are required to determine whether or not they could have collected the information under APP 3. If they determine that they could *not* have collected the personal information; the information must be destroyed.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information>.

9.2. TDIF – Overview

It is difficult to see how unsolicited information might be received by participants in the TDIF. However, it is impossible to rule this out, and APP 4 requires agencies and organisations to assess unsolicited information as it arrives, and destroy it if it is information that they could not have collected themselves.

9.3. APP 4. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

This principle on unsolicited information is not usually included in other privacy laws – it is unique to the Commonwealth APPs. However, it is likely that this principle will need to be incorporated into the TDIF Core Service Requirements.

10. APP 5. Notification of the collection of personal information

10.1. The Law

APP 5 — notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

[itemised list follows]

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>.

Note: Similar notice requirements appear in State privacy legislation.

10.2. TDIF – Overview

The TDIF is at an early stage of development, and this initial PIA is limited to a high level review of the concept and design of the TDIF and its core components.

At this early stage it is difficult to provide detailed advice on compliance with APP 5, but we can point to some key privacy issues that will be relevant to the TDIF.

The likely approach in the TDIF is that participants will be bound by the APPs or similar principles at least as strong as the APPs, through the TDIF Core Service Requirements (or possibly through legislation). This level of protection will be strengthened by regular mandatory compliance audits.

The notice requirements will clearly apply to:

- **IdPs** – at the time they enrol individuals and again when individual log in to the service to manage their identities or make an inquiry;
- **Relying Parties** – at the time they refer consumers to the Identity Exchange (Relying parties already provide notices to consumers, but may have to amend the notices to reflect (briefly) the TDIF arrangements); and
- **The Identity Exchange** – at the time consumers visit the Exchange to select an IdP for enrolment, and again at the time they visit the Exchange to select an IdP for authentication. Notices should also be provided when consumers login to access their meta-data (e.g. reviewing their recent transactions).

The appropriate content of the notices can be assessed using the following checklist:

APP 5. Notification	Action / Status	Galexia Commentary
A. Does the entity provide notice of its identity and contact details?	**To be addressed in the full PIA (2017)**	Notice will need to be provided by: • **IdPs** – at the time they enrol individuals and again when individual log in to the service to manage their identities or make an inquiry; • **Relying Parties** – at the time they refer consumers to the Identity Exchange; and • **The Identity Exchange** – at the time consumers visit the Exchange to select an IdP for enrolment, and again at the time they visit the Exchange to select an IdP for authentication.
B. Does the entity provide notice of third party collection? (if relevant)	**To be addressed in the full PIA (2017)**	Required content of the notice.
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	**To be addressed in the full PIA (2017)**	Required content of the notice.
D. Does the entity provide notice of the purpose of collection?	**To be addressed in the full PIA (2017)**	Required content of the notice.
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	**To be addressed in the full PIA (2017)**	Required content of the notice.
F. Does the entity provide notice of any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected?	**To be addressed in the full PIA (2017)**	Required content of the notice.
G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	**To be addressed in the full PIA (2017)**	Required content of the notice.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	**To be addressed in the full PIA (2017)**	Required content of the notice.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	**To be addressed in the full PIA (2017)**	Required content of the notice.

10.3. APP 5. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

The principles will definitely include notice requirements.

Recommendation 10: Notice requirements

Notice will need to be provided by:

- **IdPs** – at the time they enrol individuals and again when individual log in to the service to manage their identities or make an inquiry;
- **Relying Parties** – at the time they refer consumers to the Identity Exchange; and
- **The Identity Exchange** – at the time consumers visit the Exchange to select an IdP for enrolment, and again at the time they visit the Exchange to select an IdP for authentication.

The content of the notices will need to be determined during the full PIA (2017).

11. APP 6. Use or disclosure of personal information

11.1. The Law

APP 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information — directly related to the primary purpose; or

(ii) if the information is not sensitive information — related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or …

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

6.3 Biometric information can only be disclosed for a secondary purpose if:

the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3.[9]

There is no similar exemption for organisations (the private sector).

11.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of purpose, use and disclosure.

The Privacy hints they have identified include:

- No surprises! Use personal information in ways that are expected by the individual
- No surprises! Tell the individual about disclosures

The Privacy Risks they have identified include:

- Using personal information for unexpected secondary purposes
- Unnecessary or unexpected data linkage
- Unexpected disclosures can lead to privacy complaints

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

[9] Note: The OAIC have not yet developed the guidelines envisaged under APP 6.3 (confirmed with OAIC, 9 November 2016).

11.3. TDIF – Overview

The TDIF is at an early stage of development, and this initial PIA is limited to a high level review of the concept and design of the TDIF and its core components.

At this early stage it is difficult to provide detailed advice on compliance with APP 6, but we can point to some key privacy issues that will be relevant to the TDIF.

The likely approach in the TDIF is that participants will be bound by the APPs or similar principles at least as strong as the APPs, through the TDIF Core Service Requirements. This level of protection will be strengthened by regular mandatory compliance audits.

APP 6 divides disclosure into primary and secondary use. It is important to note that the (natural) focus of the TDIF is on disclosure for the primary uses of verifying and authenticating identity. Little attention at this early stage has been given to questions around secondary use of the data.

For primary use, the current concept and design of the TDIF is clearly compliant with APP 6. For secondary use, some further review and discussion will be required, and it is intended that this question will be assessed in the full PIA (in 2017).

One aspect of secondary use that has been the subject of some limited consideration is the potential secondary use of data by third parties in relation to identity fraud and suspicious transactions.

The use of data to investigate identity fraud and suspicious transactions might require access to the meta-data held by the Identity Exchange, the enrolment data and logs held by IdPs, and the transaction data and logs held by relying parties. In more serious or more complex investigations, data from several sources could be required. It is anticipated that investigation of identity fraud or suspicious transactions could be triggered by users, TDIF participants or third parties.

It may not be necessary for every case of identity fraud or suspicious transactions to be formally investigated by a law enforcement agency. TDIF participants themselves may wish to review some transactions or to assist consumers investigate suspicious activity. Obviously some patterns of identity fraud may be detected by broad data collection (not requiring individual consumer names), but more complex investigations will require the sharing of personal data.

The exact scope and rules for the investigation of identity fraud and suspicious transactions by TDIF participants should be addressed in the TDIF Core Service Requirements and other TDIF documentation. The extent of this secondary use should be disclosed to consumers.

The following table summarises the key compliance tasks relevant to APP 6:

Use or Disclosure (APP 6)	Action / Status	Galexia Commentary
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	**To be addressed in the full PIA (2017)**	At this early stage the discussion of the TDIF has concentrated on the two main primary uses of the data – the initial enrolment followed by ongoing authentication. There has been no decision and only limited discussion on secondary use of the data. Stakeholders were obviously very keen to restrict secondary use as far as possible, although views differed on the appropriate mechanism for achieving this result.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)?	**To be addressed in the full PIA (2017)**	There has been no decision and only limited discussion on secondary use of the data.

Use or Disclosure (APP 6)	Action / Status	Galexia Commentary
C. Is any biometric information only disclosed for a secondary purpose in accordance with Clause 6.3 and the relevant OAIC Guidelines?	**Requires further review / action**	APP 6 provides some additional rules for the secondary use and disclosure of biometric data. However, the detailed provisions are delegated to 'guidelines' which have not yet been developed. In the meantime, the TDIF Core Service requirements should incorporate some additional privacy protections for the use of biometric data in the TDIF. These should include (at least): 1. A strict prohibition on the biometric data being used for any secondary purpose (i.e. it would be restricted to verification of a photograph during initial enrolment); 2. A requirement for all biometric data to be destroyed once the photograph has been verified (this is already a requirement of the draft TDIF Digital ID Verification Standard); and 3. The extension of these rules to all TDIF participants (APP 6.3 only applies to government agencies).
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	**Requires further review / action**	The legal requirement to make a written note of law enforcement related disclosures is a very minimal standard that does little to address community concerns regarding law enforcement access and potential government surveillance. This is an area where the TDIF Core Service Requirements could help to strengthen privacy protections, beyond the very limited requirements in the Privacy Act. Emerging best practice is for organisations to issue annual 'transparency reports' that disclose the broad scale and scope of access requests by law enforcement agencies.

11.4. APP 6. Finding

At this early stage in the development of the TDIF it is difficult to provide detailed advice on compliance with APP 6, but we can point to some 3 key privacy issues that will be relevant to the TDIF:

- Secondary use for investigating identity fraud;
- Use of biometric data; and the
- Development of a transparency report regarding law enforcement access.

Recommendation 11: Secondary use for investigating identity fraud and suspicious transactions

The exact scope and rules for the investigation of identity fraud and suspicious transactions by TDIF participants should be addressed in the TDIF Core Service Requirements and other TDIF documentation. The extent of this secondary use should be disclosed to consumers.

Recommendation 12: Use of biometric data

APP 6 provides some additional rules for the use and disclosure of biometric data. However, the detailed provisions are delegated to 'guidelines' which have not yet been developed. In the meantime, the TDIF Core Service requirements should incorporate some additional privacy protections for the use of biometric data in the TDIF. These should include (at least):

A. A strict prohibition on the biometric data being used for any secondary purpose (i.e. it would be restricted to verification of a photograph during initial enrolment);
B. A requirement for all biometric data to be destroyed once the photograph has been verified; and
C. The extension of these rules to all TDIF participants (APP 6.3 only applies to government agencies).

Recommendation 13: Development of a transparency report

APP 6 requires entities to keep a written note of third party access to data by law enforcement agencies. This is an area where the TDIF Core Service Requirements could help to strengthen privacy protections, beyond the very limited requirements in the Privacy Act. Emerging best practice is for organisations to issue annual 'transparency reports' that disclose the broad scale and scope of access requests by law enforcement agencies. The TDIF should adopt this approach and publish a regular transparency report.

12. APP 7. Direct marketing

12.1. The Law

APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-7-app-7-direct-marketing>.

12.2. TDIF – Overview

This APP will not be relevant in the TDIF project. However, there may be an opportunity to clarify that direct marketing is not permitted by including a prohibition in the privacy principles in TDIF legislation (if any) or the TDIF Core Service Requirements.

12.3. APP 7. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

Under either option, the use of TDIF personal data for direct marketing should be prohibited.

Recommendation 14: Direct marketing prohibition

The use of TDIF personal data for direct marketing should be prohibited in the privacy principles in the TDIF Core Service Requirements.

13. APP 8. Cross-border disclosure of personal information

13.1. The Law

APP 8 states that before an organisation discloses personal information to an overseas recipient, they must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. The organisation that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient. Several exceptions apply.

APP 8 — Cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) *[several additional exceptions apply, but it is difficult to see how these will be relevant in the TDIF]*

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.

13.2. TDIF – Overview

The TDIF is in the early stages of development, but there is considerable opportunity for the cross border transfer of data. This will mainly occur due to hosting and platform arrangements for IdPs and the Identity Exchange, which potentially could run on cloud services provided by third parties.

Most cloud services can now help clients limit the overseas transfer of data, for example by offering a local host server in Australia, but there is no intention at this stage to limit TDIF participants to using local servers.

The main restriction on the cross border transfer of data *outside Australia* is therefore APP 8 in the Privacy Act, or its equivalent, or its equivalent provisions in the final Core Service requirements (when they are developed).

In addition to the transfer of data outside Australia, the TDIF Core Service Requirements may also have to address the issue of the cross-border transfer of data within Australia (e.g. between States).

Most State privacy regulators are concerned about the transfer of data held by local agencies outside their jurisdiction, especially if there is a chance that the data will then be used or disclosed in a jurisdiction that does not have a strong privacy law or an independent data protection regulator (such as South Australia and Western Australia).

The law varies from state to state, but the level of concern is uniformly high.

The DTA is considering addressing this issue, in part, by developing a consistent set of privacy principles (in the TDIF Core Service Requirements) that meet or exceed the highest standards in each jurisdiction. For example, if a state privacy principles on a specific issue is the highest standard in Australia on that issue, then it would become the TDIF privacy requirement. The result of such an approach is that a TDIF entity (such as an IdP) would meet or exceed the standard of privacy protection required no matter where the data was held in Australia.

This approach has some support from stakeholders, although questions still remain about the detailed principles and the appropriate mechanism for enforcement and oversight. It should be noted that there is some opposition to this approach, largely from regulators who fear that organisations may end up having split responsibilities and inconsistent privacy principles applying to different parts of their business.

This PIA recognises that privacy protection in a federation like Australia is complex and challenging, and that the data in the TDIF is likely to be transferred across numerous borders both within and outside Australia. The DTA proposal to establish a high bar for privacy protection that meets or exceeds all current requirements is a worthwhile proposal, and should be explored further. Stakeholders expect to be consulted on the detailed provisions and the enforcement and oversight mechanism.

In addition, considerable work will be required on identifying and mapping cross border transfers, in order to ensure that all transfers are the subject of appropriate notice to consumers, protection and ongoing oversight and review.

Cross-border Disclosure (APP 8)	Action / Status	Galexia Commentary
A. Has the entity identified all relevant cross border disclosure of personal information?	**Requires further review / action**	Each TDIF participant will be required to identify and map all cross-border data transfers (including both inside and outside Australia). This information will be important in order to comply with the notice requirements (see APP 5 for more details) and the protection requirements (see below).

Cross-border Disclosure (APP 8)	Action / Status	Galexia Commentary
B. Has the entity taken such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs? (unless a relevant exception applies)	**Requires further review / action**	It is likely that the key transfers will be the transfer of data to cloud service platforms that may be hosted overseas, and the transfer of data amongst TDIF participants, where the original data is held by a state entity that is subject to a cross border data transfer restriction (within Australia). APP 8 allows entities to choose whether they wish to take direct steps to ensure the data is protected, or to rely on one of the broad exceptions. The most relevant exception is where the receiving entity is covered by similar laws to the Privacy Act, and consumers have a right of redress. State laws provide slightly different rules and exceptions. It may be necessary for the TDIF to develop a uniform approach to all cross-border transfers in order to ensure a consistent level of protection and assurance. This PIA is not suggesting that cross-border data transfers should be prohibited (it is likely that some of the most effective and innovative providers of Identity related services may include an element of offshore support or hosting), but it does recommend that a strong, uniform requirement for protecting privacy in such transfers is added to the TDIF Core Service requirements. In practice, APP 8 would allow TDIF entities to pursue three completely different courses for protecting cross border transfers – direct action / responsibility, reliance on 'substantially similar' protection, or explicit consent. This may lead to significant divergence in the level of protection provided to individuals. The TDIF Core Service requirements should endeavour to 'raise the bar' on this issue. They could, for example, disallow reliance on 'substantially similar' protection or consent, and instead provide guidance on mechanisms to take direct action / responsibility.

13.3. APP 8. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

There is some expectation that a consistent set of privacy principles can be developed, and that this would help to lift the standard of privacy protection in the TDIF. However, in the area of cross-border data transfers this requires considerable further work.

In the Commonwealth Privacy Act APP 8 allows organisations to pursue three completely different approaches to protecting privacy.

- Entities can choose to take direct action (and responsibility). In the TDIF this could take the form of direct privacy provisions in contracts with service providers, backed up by audit and assurance regimes.
- Entities can choose to rely on 'substantially similar protections in the receiving jurisdiction, accompanied by the ability for consumers to have redress in that jurisdiction.
- Entities can choose to rely on explicit notice and explicit consent

In this PIA we caution against allowing this flexible approach to protecting privacy in cross-border transfers. These transfers are going to be common, and the TDIF already envisages parties operating in a number of jurisdictions. Allowing further flexibility, similar to the options in APP 8, will lead to complexity and an inconsistent level of protection for individuals.

The TDIF should insist on a single approach to protecting privacy in the case of cross border data transfers. This approach should be set out in detail in the TDIF Core Service requirements, following further consultation with stakeholders.

The following two recommendations relate to cross-border data transfers *overseas*. Some further discussion of cross-border data transfers amongst Australian jurisdictions will be included in the full PIA (2017).

Recommendation 15: Cross border data transfer – Mapping

Each TDIF participant should identify and map their cross-border data transfers. This is an important step in meeting the (expected) notice and protection provisions in the TDIF Core Service Requirements

Recommendation 16: Cross border data transfer – Protection

Cross border data transfers in the TDIF should be permitted subject to the development of a single, consistent mechanism for protecting privacy in such transfers. The protection mechanism should be included in the TDIF Core Service Requirements. For the avoidance of doubt the protection mechanism could be both stronger and less flexible than the approaches permitted in current privacy law (particularly APP 8 in the Commonwealth Privacy Act), in order to meet the objective of consistent privacy protection throughout the TDIF.

14. APP 9. Adoption, use or disclosure of government related identifiers

14.1. The Law

APP 9 states that an organisation must not adopt a government related identifier of an individual as its *own* identifier. In addition, an organisation must not use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual. Some other exceptions apply.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers>.

14.2. TDIF – Overview

APP 9 contains two key requirements.

The first is that organisations must not adopt a government identifier as their own identifier. This is designed to prevent the development of de facto national identifiers. For example, organisations cannot use the Tax File Number (issued by the Commonwealth government) as their own identifier.

In the TDIF, a number of government related identifiers will be temporarily utilised in the process of verifying individuals, but there is no intention of any participant adopting one of these identifiers as their own.

The prohibition on adoption should apply to all TDIF participants, through the development of a principle in the TDIF Core Service Requirements.

The second requirement of APP 9 is that government related identifiers should not be disclosed except in specific situations where the disclosure is reasonably necessary to verify identity. Obviously the entire purpose of the TDIF is to verify identity, and identifiers can be shared for this purpose. However, the restriction will place a useful 'limit' on the disclosure of identifiers for unrelated purposes.

In practice, the TDIF allows IdPs to also develop a new identifier. This identifier could take many forms, but for most IdPs it is likely to be a GUID (a global unique identifier) that can be used to ensure uniqueness amongst records with similar content (e.g. individuals with common names). These identifiers will be 'government related identifiers' for the purpose of APP 9 - "a government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract".

Therefore, the restrictions on adoption by other organisations and disclosure will apply.

This is a useful layer of privacy protection for these identifiers. However, stakeholders were very concerned about the development of these identifiers by IdPs. They share some similarities with previous proposals for national identity numbers (e.g. the Australia Card and the Access Card), and although there was no current intention to use the identifiers outside individual IdPs, stakeholders believed that there would be considerable potential function creep or scope creep once the identifiers were created.

It is difficult to completely eliminate the development of identifiers in a verification framework where uniqueness is important. Protection against misuse will have to be provided through a combination of factors:

- Prohibition on adoption of the identifier by other organisations;
- Prohibition on disclosure of the identifier apart from specific situations where it is necessary to verify identity;
- Confirmation (possibly in legislation) that identifiers in the TDIF are not to be used for purposes outside the TDIF;
- Confirmation that consumers will always have a choice of more than one IdP in any TDIF transaction;

14.3. APP 9. Finding

The TDIF will result in IdPs developing new identifiers in order to uniquely identify their clients. APP 9 does not provide a sufficient level of privacy protection in relation to these identifiers. The TDIF Core Service requirements should therefore be strengthened to incorporate additional protections in relation to IdP identifiers.

Recommendation 17: Restriction on the use of IdP identifiers

Unique identifiers developed by IdPs should not be adopted by any third party as their identifier and the disclosure of IdP identifiers should be severely restricted to specific situations requiring verification of identity.

Recommendation 18: Additional restriction on IdP identifiers

In order to prevent function creep and scope creep (as far as possible) in relation to the use of IDP identifiers, the TDIF should adopt measures to ensure that identifiers in the TDIF are not to be used for purposes outside the TDIF. In addition, measures should be implemented to ensure that consumers will always have a choice of more than one IdP in any TDIF transaction.

15. APP 10. Quality of personal information

15.1. The Law

APP 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

15.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of data quality.

The Privacy Risks they have identified include:

- Retaining personal information unnecessarily
- Making decisions based on poor quality data

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-10-app-10-quality-of-personal-information>.

15.3. TDIF – Overview

The current TDIF concept and design include a range of measures to ensure data quality. These include:

- Verifying identity documents using the DVS;
- Verifying photographs using the FVS;
- Requiring each IdP to prevent / remove duplicate records.

At the same time, there are other Government led initiatives around Australia to improve the quality of data utilised in identity verification processes. These include upgrades to systems and digital records at key data custodians (e.g. Registries of Births, Deaths and Marriages) and improvements to the quality of photographs collected and held by state driver licence agencies.

Some further work is being undertaken on related data quality issues, such as the time periods for validity and renewal of identities – noting that it is important that identity data is up to date having regard to the purpose of the use or disclosure.

Issues to consider in the TDIF in relation to data quality include:

- How frequently photographs should be refreshed;
- Action to be taken when core data fields change – noting that the current model envisages IdPs collecting mobile phone and email data (which may change regularly); and
- Action to be taken for formal changes of name.

This initial PIA has not considered data quality issues in detail.

APP 10. Data Quality	Action / Status	Galexia Commentary
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information collected is accurate, up-to-date and complete?	**Current design is compliant**	The current TDIF concept and design include a range of measures to ensure data quality. These include: ● Verifying identity documents using the DVS; ● Verifying photographs using the FVS; ● Requiring each IdP to prevent / remove duplicate records.
B. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **that the entity uses or discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant?	**Requires further review / action**	Some further work is being undertaken on related data quality issues, such as the time periods for validity and renewal of identities. It is important that identity data is up to date having regard to the purpose of the use or disclosure – this may have an impact on the appropriate time periods for refreshing key data.

15.4. APP 10. Finding

The current TDIF concept and design include a range of measures to ensure data quality, but this initial PIA has not considered data quality issues in detail.

Some further work is being undertaken on related data quality issues, such as the time periods for validity and renewal of identities – noting that it is important that identity data is up to date having regard to the purpose of the use or disclosure.

16. APP 11. Security of personal information

16.1. The Law

APP 11 requires organisations to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

Also, if the organisation no longer needs the information for any purpose for which the information may be used or disclosed, they must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

16.2. OAIC Guidelines

APP 11 has a very wide scope for interpretation, as it includes multiple tests for what is 'reasonable in the circumstances'. Some additional guidance is available from the Office of the Australian Information Commissioner (OAIC) in the form of guidelines:

- *Guide to securing personal information*, OAIC, 2015 <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

16.3. TDIF Overview

The TDIF is being developed during a period of significant community concern regarding security and cybersecurity. Many agencies and organisations in Australia and elsewhere have been the subject of high profile attacks resulting in data breaches.

APP 10 in the Privacy Act is only a small component of the broader security compliance framework that will apply to the TDIF. The key to complying with APP 10 is to implement security measures that are in proportion to the risk and impact of a breach of the data held in the TDIF.

In order to implement these measures, the Privacy Commissioner recommends that entities undertake a risk assessment.

In the recent Ashley Maddison case (concerning a significant data breach) the Privacy Commissioner stated:

> Conducting regular and documented risk assessments is an important organizational safeguard in and of itself, which allows an organization to select appropriate safeguards to mitigate identified risks and reassess as business and threat landscapes change. Such a process should be supported by adequate external and/or internal expertise, appropriate to the nature and volume of personal information held and the risks faced.[10]

During this PIA, stakeholders queried the potential use of encryption in the TDIF. At this early stage of development, the extent to which data is encrypted in the TDIF is unclear. The TDIF Core Service Requirements will ultimately establish rules for the encryption of data (in storage and in transit).

Stakeholders also queried the potential use of authentication apps provided by third parties (e.g. Google Authenticator). These apps can often complement or replace the use of one time passwords or tokens sent by mobile phone. Again, at this early stage of development, the extent to which data is encrypted in the TDIF is unclear. The TDIF Core Service Requirements will ultimately establish rules for the encryption of data (in storage and in transit).

[10] Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner (September 2016), <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison>

Most of the security arrangements for the TDIF are not yet developed, or are too detailed to be included in this initial PIA, but it is important that these issues are addressed. Security issues have therefore been added to the Future Work Plan (see section 20 towards the end of this PIA).

Security is also likely to be a fairly dynamic component of the TDIF, with constant reviews and upgrades, rather than being based on security settings that are prescribed from the first day of operation.

Security (APP 11)	Action / Status	Galexia Commentary
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss?	**To be addressed in the full PIA (2017)**	Security arrangements for the TDIF are under development, and are not covered in detail in this initial PIA.
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	**To be addressed in the full PIA (2017)**	Security arrangements for the TDIF are under development, and are not covered in detail in this initial PIA.
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	**To be addressed in the full PIA (2017)**	Security arrangements for the TDIF are under development, and are not covered in detail in this initial PIA.
D. Will detailed access trails be retained and scrutinised for security breaches?	**To be addressed in the full PIA (2017)**	Security arrangements for the TDIF are under development, and are not covered in detail in this initial PIA.
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	**To be addressed in the full PIA (2017)**	Security arrangements for the TDIF are under development, and are not covered in detail in this initial PIA.
F. Is personal information de-identified as soon as possible?	**To be addressed in the full PIA (2017)**	Security arrangements for the TDIF are under development, and are not covered in detail in this initial PIA.
G. Is a data breach response plan in place?	**To be addressed in the full PIA (2017)**	This is currently a voluntary requirement (OAIC Data breach notification guide, 2014), but there is legislation before parliament to introduce mandatory data breach notification requirements.

16.4. APP 11. Finding

Most of the security arrangements for the TDIF are not yet developed. Detailed security requirements have not been considered in this initial PIA.

17. APP 12. Access to personal information

17.1. The Law

APP 12 — access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exceptions to access…

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

17.2. TDIF – Overview

Access requests may cause some difficulties in the TDIF, as multiple participants may each hold part of the relevant data.

The Identity Exchange will only hold limited personal data, but it will retain metadata on each transaction. The IdPs will hold the most complete set of data, but will not hold any information on the eventual use of the data (as this is masked by the Identity Exchange).

Consumers may make a general access request to any participant in the TDIF. For example, even though the Identity Exchange only holds limited personal data, the operators of the Identity Exchange may still receive some consumer access requests, and it will be important to make the access request process 'clear and straightforward' for consumers. This may require TDIF participants to collaborate (e.g. provide a collective response), or to make appropriate referrals to each other.

Finally, there is some inconsistency in the APPs in relation to access requests – different rules apply to agencies (government) and organisations (the private sector). In order to ensure a consistent experience for consumers, all TDIF participants should be required to meet the higher access standards (set out in the table below).

APP 12. Access	Action / Status	Galexia Commentary
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	**Current design is compliant**	Privacy policies will be adopted that clearly identify the nature (and scope) of personal information held by TDIF participants and the access methods available.
B. If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply)	**Requires further review / action**	Two distinct access 'paths' in the TDIF: • **Path 1: The Identity Exchange** - The Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transaction or identity fraud. - The number of transactions (or period) is yet to be determined (refer to section 4.2 for further details). - This type of access would need to be carefully managed to prevent unauthorised access. • **Path 2: IdPs** - Each IdP will need to offer access to all the records that it holds on an individual, without restriction. - Again, access would need to be carefully managed to prevent unauthorised access.

APP 12. Access	Action / Status	Galexia Commentary
C. Will information be provided within 30 days?	**Requires further review / action**	In the Commonwealth Privacy Act the 30 day requirement only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants (including the private sector) to ensure a consistent experience for consumers.
D. Will accessing personal information be provided at no cost?	**Requires further review / action**	In the Commonwealth Privacy Act the free access requirement only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants (including the private sector) to ensure a consistent experience for consumers.

17.3. APP12. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

The TDIF Core Service Requirements should ensure that the Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transaction or identity fraud. In addition, each IdP will need to offer access to all the records that it holds on an individual, without restriction.

Recommendation 19: Access requests – Application in the TDIF

The TDIF Core Service Requirements should ensure that the Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transaction or identity fraud. In addition, each IdP will need to offer access to all the records that it holds on an individual, without restriction.

In addition, some parts of APP 12 should be strengthened in the TDIF Core Service requirements in order to provide a consistent experience for consumers.

Recommendation 20: Access requests – Consistency

In the Commonwealth Privacy Act the requirement that access will be provided within 30 days only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants (including the private sector) to ensure a consistent experience for consumers. Similarly, the 'free access' requirement only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants.

18. APP 13. Correction of personal information

18.1. The Law

APP 13 — correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

…

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency — within 30 days after the request is made; or

(ii) if the entity is an organisation — within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

18.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of correction of personal information.

- Getting access to personal information should be clear and straightforward.
- Inaccurate information can cause problems for everyone!

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-13-app-13-correction-of-personal-information>.

18.3. TDIF – Overview

Complaints and correction requests may cause some difficulties in the TDIF, as multiple participants may each hold part of the relevant data. The responsibility for complaints may be difficult to determine, and the complaints 'pathway' for consumers may be complex.

Also, it is important for all TDIF participants to learn from complaints, so some sharing of complaints and complaints data across the TDIF will be useful.

The Identity Exchange may only play a limited role in relation to complaints, but some consumers may approach the Identity Exchange with their complaints in situations where they are not sure who is responsible. IdPs and Relying parties will also be approached in relation to TDIF complaints.

It will be important to make the complaints and correction process 'clear and straightforward' for consumers. This may require TDIF participants to collaborate (e.g. provide a collective response), or to make appropriate referrals to each other.

Finally, there is some inconsistency in the APPs in relation to complaints – different rules apply to agencies (government) and organisations (the private sector). In order to ensure a consistent experience for consumers, all TDIF participants should be required to meet the higher complaints standards (set out in the table below).

APP13. Correction	Compliant	Galexia Commentary
A. UPON REQUEST Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	**Current design is compliant**	The TDIF Core Service Requirements will include a process for correcting inaccurate data.
B. UPON LEARNING OF INACCURACIES Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	**Current design is compliant**	The TDIF Core Service Requirements will include a process for correcting inaccurate data.
C. UPON REQUEST ONLY Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	**To be addressed in the full PIA (2017)**	The TDIF Core Service Requirements will need to include a process for disseminating corrections to TDIF data amongst participants. This is a complex issue and it has not been considered in detail in this initial PIA.
D. UPON REQUEST ONLY Will the entity take such steps as are reasonable in the circumstances to associate a statement by the data subject that the accuracy of the information is challenged in such a way that will make the statement apparent to users of the information?	**To be addressed in the full PIA (2017)**	The TDIF Core Service Requirements will need to include a process for allowing annotations to be made to TDIF data. This requirement presents some significant technical challenges. This is a complex issue and it has not been considered in detail in this initial PIA.
E. Will requests for corrections be addressed within 30 days?	**Requires further review / action**	In the Commonwealth Privacy Act the 30 day requirement only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants (including the private sector) to ensure a consistent experience for consumers.

18.4. APP 13. Finding

The TDIF may be subject to specific privacy principles in legislation – the governance arrangements for the TDIF are still under development. In any case, participants will be subject to the TDIF Core Service Requirements, and these will contain a set of standard privacy principles.

Complaints and correction requests may cause some difficulties in the TDIF, as multiple participants may each hold part of the relevant data. The responsibility for complaints may be difficult to determine, and the complaints 'pathway' for consumers may be complex.

Also, it is important for all TDIF participants to learn from complaints, so some sharing of complaints and complaints data across the TDIF will be useful.

Recommendation 21: Complaints coordination

It will be important to make the complaints and correction process 'clear and straightforward' for consumers. This may require TDIF participants to develop an appropriate referrals service. In addition, some data on complaints should be shared across the TDIF to ensure participants learn from complaints.

There is some inconsistency in the APPs in relation to complaints – different rules apply to agencies (government) and organisations (the private sector). In order to ensure a consistent experience for consumers, all TDIF participants should be required to meet the higher complaints standards.

Recommendation 22: Complaints – Consistency

In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints within 30 days.

19. Governance

The DTA has recently commissioned an independent report on governance arrangements for the TDIF – "all options are on the table", and the DTA recognises the importance of governance in relation to privacy protection in the TDIF. The report will recommend governance models for the Federation (another consultancy relating to development of those rules will be issued once the options have been considered).

The question of governance was raised by all stakeholders during this initial PIA.

It is beyond the scope of this initial PIA to provide comprehensive advice on governance, but this issue will be revisited in the full PIA (2017). At that time a full governance proposal will be available from the DTA.

However, some key high level principles on governance have emerged during the initial PIA, and these could be included in the DTA governance review. This section briefly summarises the key suggestions.

19.1. Structural separation

From a privacy perspective, it will be important to ensure that complete structural separation is achieved between the Identity Exchange and any IdPs. This includes the proposed Commonwealth IdP.

This structural separation is an important privacy protection as the intention is that IdPs will not have any visibility of data in the Identity Exchange (and vice versa). This assurance could not be provided if the IdP and Identity Exchange are being managed by the same entity.

The current approach is that the DTA will play a role in developing both the Identity Exchange and the Commonwealth IdP, at least in the early stages of development. This dual role is not sustainable once the Framework goes live. One of the components – either the IdP or the Identity Exchange – will need to be 'spun off' to become a separate entity or transferred to the responsibility of another entity.

The governance documentation being developed by the DTA should specify a complete structural separation between IdPs and the Identity Exchange, including a roadmap for achieving this outcome.

19.2. Independent accreditation

From a privacy perspective, it will be important to ensure confidence in the accreditation process, including integrity and a level playing field for all participants.

It is therefore vital that the accreditation body for the TDIF should be completely separate from any IdPs. The governance report could look at other federated models in other sectors for the best model to achieve this outcome.

It is essential from a privacy perspective that the privacy principles in the Core Service Requirements are 'policed' by a separate entity to the TDIF participants (e.g. IdPs and the Identity Exchange). This may present some challenges for the DTA which needs to play a leadership role and 'drive' quality improvements in digital identity, but the separation and independent assessment is essential.

19.3. Legal authority

Numerous stakeholders in this initial PIA raised concerns about the lack of underlying legal authority for the establishment of the TDIF. From the perspective of this initial PIA, we note that the establishment of legal authority is not a solution itself to many of the privacy issues that have been identified.

There were mixed views from stakeholders on the best model for establishing legal authority. A real concern amongst some stakeholders was that greater legal authority (e.g. the development of legislation) might favour surveillance over privacy, and that 'consideration by parliament' is no longer associated with the assurance of privacy protection.

The DTA acknowledges that governance arrangements are a key aspect of the TDIF and has commissioned further work on developing a governance model. One concern is that, to the extent that there needs to be legal authority, care needs to be taken to avoid prescribing authentication standards, data storage, and other standards that might be unable to keep pace with the changing nature of digital verification and authentication. One option is to establish a 'light touch' legal authority that allows the Federation - which is proposed to contain non-government entities - to set the standards.

19.4. Complaints and access requests

As discussed in APP 12 and APP 13 above, there is potential for coordination between TDIF participants in relation to access and correction requests. This would assist consumers find a clearer path for their requests, and help all TDIF participants to learn important lessons from complaints (rather than that information remaining in silos).

The governance report being commissioned by the DTA could consider the structure or mechanism to achieve this result in practice.

19.5. TDIF participant membership / engagement

All stakeholders were of the view that if an entity joins the TDIF they should have an appropriate level of membership or engagement. Suggestions for addressing this varied, but included:

- The development of a co-operative;
- Provision of a 'seat at the board';
- Development of a COAG agreement; and
- Establishment of a national digital identity task force.

Many stakeholders were unwilling to have the rules for digital identity 'imposed from above' without the opportunity for input, collaboration and an ongoing role in oversight.

Stakeholders also suggested that governance arrangements should incorporate consumer engagement. This could take the form of a policy advisory committee. Similar models operate in other sectors (such as the ACCC Consumer Consultative Committee and the ASIC Consumer Advisory Panel).

Stakeholders saw benefits in regular 'baked in' reviews & evaluations, including mandatory public consultation.

Recommendation 23: Governance arrangements

The DTA has recently commissioned a report on governance arrangements for the TDIF. The report should consider the following key governance issues (that have a direct impact on privacy protection):

A. Ensuring complete structural separation between the Identity Exchange and IdPs;
B. Ensuring an independent process is in place for TDIF accreditation;
C. Developing an appropriate underlying legal authority for the TDIF;
D. Developing appropriate coordination mechanisms for access and correction requests amongst TDIF participants, including the ability to share complaints data; and
E. Developing an appropriate mechanism for TDIF membership and ongoing engagement with stakeholders.

20. Recommended Future Privacy Work Plan

This PIA has made a range of recommendations to address privacy concerns. Many of these recommendations require the DTA (and its providers) to undertake specific tasks or to make changes to documents or processes that were already under development. The following table summarises the key implementation steps (and responsibilities) that arise from this PIA:

Recommendation	Action Required	Person / Agency responsible	Method of Verification
Issue – Component 1: TDIF policies and standards			
R1: The TDIF accreditation / revocation proposal	Clarify and explain the detailed powers behind this proposal	DTA	Full PIA 2017
R2: Privacy principles in the Core Service Requirements	Develop a set of draft Privacy Principles and consult with stakeholders	DTA	Full PIA 2017
Issue – Component 2: The Identity Exchange			
R3: The Identity Exchange and the retention of metadata	Determine a specific meta-data retention period	DTA	Full PIA 2017
R7: The Identity Exchange and the definition of Personal Information	The Identity Exchange documentation should classify all data as personal information.	DTA	Draft Identity Exchange documentation
R8: Openness Task	The Identity Exchange should develop a specific privacy policy	DTA	Draft Identity Exchange documentation
R10: Notice requirements	Develop notices to be provided by the Identity Exchange at the time consumers visit the Exchange to select an IdP for enrolment, and again at the time they visit the Exchange to select an IdP for authentication.	DTA	Full PIA 2017
R19: Access requests – application in the TDIF.	The TDIF Core Service Requirements should ensure that the Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transaction or identity fraud.	DTA	Draft TDIF Core Service Requirements
R22: Complaints – Consistency	In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints within 30 days	DTA	Draft TDIF Core Service Requirements
Issue – Component 3: Identity Providers (IdPs)			
R4: The selection of a single Commonwealth IdP – further consultation	Further stakeholder engagement (workshop / consultation)	DTA	Full PIA 2017
R5: The selection of a single Commonwealth IdP – risk assessment	Completion of a detailed risk assessment	Independent provider	Full PIA 2017
R6: Identity Providers and the definition of Personal Information	The TDIF Core Service Requirements should classify all data used by Identity Providers (IdPs) as Personal Information.	DTA	Draft TDIF Core Service Requirements
R8: Openness task	Specific requirements on openness and transparency should be set out in the TDIF Core Service Requirements	DTA	Draft TDIF Core Service Requirements
R9: Collection of sensitive data	The next iteration of the TDIF design will need to incorporate specific explicit consent from users to the collection of biometric data at the enrolment stage	DTA	Full PIA 2017

Recommendation	Action Required	Person / Agency responsible	Method of Verification
R10: Notice requirements	Develop notices to be provided by IdPs at the time they enrol individuals and again when individuals log in to the service to manage their identities or make an inquiry	IdPs	Full PIA 2017
R14: Direct marketing prohibition	The use of TDIF personal data for direct marketing should be prohibited in the TDIF Core Service Requirements	DTA	Draft TDIF Core Service Requirements
R17: Restriction on the use of IdP identifiers	The TDIF Core Service Requirements should state that unique identifiers developed by IdPs should not be adopted by any third party as their identifier and the disclosure of IdP identifiers should be severely restricted to specific situations requiring verification of identity.	DTA	Draft TDIF Core Service Requirements
R18: Additional restriction on IdP identifiers	Additional restrictions and guarantees should be implemented to prevent function creep and scope creep in relation to IdP identifiers.	DTA	Full PIA 2017
R19: Access requests – application in the TDIF.	Each IdP will need to offer access to all the records that it holds on an individual, without restriction.	DTA / IdPs	Draft TDIF Core Service Requirements
R20: Access requests – consistency	The TDIF Core Service Requirements should adopt common access requirement across all IdPs.	DTA	Draft TDIF Core Service Requirements
R22: Complaints – Consistency	In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints within 30 days	DTA	Draft TDIF Core Service Requirements
Issue – Overall Program			
R11: Secondary use for investigating identity fraud and suspicious transactions	The exact scope and rules for the investigation of identity fraud and suspicious transactions by TDIF participants should be addressed in the TDIF Core Service Requirements and other TDIF documentation.	DTA	Full PIA 2017
R12: Use of biometric data	The TDIF Core Service Requirements should incorporate some additional privacy protections for the use of biometric data.	DTA	Draft TDIF Core Service Requirements
R13: Development of a transparency report	The TDIF should publish an annual transparency report on law enforcement access.	DTA	Full PIA 2017
R15: Cross border data transfer – mapping	Each TDIF participant should identify and map their cross-border data transfers.	DTA / IdPs	Ongoing
R16: Cross border data transfer – protection	The TDIF Core Service Requirements should include stronger and more consistent principles on cross border disclosures.	DTA	Draft TDIF Core Service Requirements
R21: Complaints coordination	It will be important to make the complaints and correction process 'clear and straightforward' for consumers. This may require TDIF participants to develop an appropriate referrals service. In addition, some data on complaints should be shared across the TDIF to ensure participants learn from complaints.	DTA	Full PIA 2017
R23: Governance arrangements	The DTA has recently commissioned a report on governance arrangements for the TDIF. The report should consider several issues raised in the initial PIA.	Independent provider	Draft Governance report

21. Appendix 1 – Stakeholder Consultation

The following meetings were held with key stakeholders:

- Australia Post
- Australian Communications Consumer Action Network (ACCAN)
- Australian Privacy Foundation (APF)
- Commissioner for Privacy and Data Protection Victoria (CPDP)
- Department of Finance, Services and Innovation NSW (DFSI)
- Digital Rights Watch
- Information and Privacy Commission NSW (IPC)
- Office of the Australian Information Commissioner (OAIC)
- Office of the Information Commissioner QLD (OIC)
- Queensland Government Chief Information Office (QGCIO)
- Queensland SmartService (Digital Productivity and Services Division)
- Service NSW

22. Appendix 2 – Background Information

The following documents have been supplied by DTA for consideration in this document:

Trusted Digital Identity Framework Document	Purpose
Overview v0.2 – August 2016	This document provides an overview of the Framework – what it is; why it's needed; how it's being developed; who's involved; what's been developed so far, and what is yet to be developed
Digital Identity Risk Management Standard v0.2 – August 2016	The Digital Identity Risk Management Standard sets out a risk management process based on AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines. The Standard provides a consistent manner for federated digital identity participants to follow, in order to establish their identity assurance requirements and mitigate risks. This document details the process Participants must follow to complete their digital identity risk assessment.
Digital Identity Verification Standard v0.6 – August 2016	This Digital Identity Verification Standard sets out the requirements for the verification of an individual's identity that need to be met by entities accredited as Identity Providers (IdPs) under the Framework.
Digital Authentication Credential Standard v0.3 – August 2016	This Digital Authentication Credential Standard ('the Standard') sets out the requirements relating to authentication credentials, their issuance and lifecycle management that need to be met by entities accredited as Credential Providers under the Framework.
Core Service Requirements v0.6 – August 2016	The Core Service Requirements (CSRs) define a baseline of the privacy, protective security and accessibility, usability and inclusive design activities for accredited Service Providers to complete in order be accredited against the Framework..
Federated Identity Architecture v0.2 – August 2016	The Trusted Digital Identity Framework ('Trust Framework') employs a federation-style approach for the identity 'eco-system'. This document describes the components of the identity federation including the information flows, the protocols and assertions.
Memorandum of Agreement Template v0.3 – August 2016	This document is a draft template agreement between participants in the Framework.
Glossary of Terms v0.2 – August 2016	This document is a glossary of common terms used in the Framework.
Digital Identity – Individuals (Architecture) v0.4 – October 2016	This document describes the initial architecture for an Australian Digital Identity platform. The fundamentals of the architecture are detailed and some of the fundamental design decisions elaborated on.

23. Appendix 3 – Acronyms

Acronym	Term	Reference
ACCC	Australian Competition and Consumer Commission	https://www.accc.gov.au
APP	Australian Privacy Principle	https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/
COAG	Council of Australian Governments	http://www.coag.gov.au
DTA	Digital Transformation Agency	https://www.dta.gov.au
DTO	Digital Transformation Organisation	DTO transitioned to the DTA in October 2016
DVS	Document Verification Service	http://www.dvs.gov.au
EOI	Evidence of Identity	
FVS	Face Verification Service	https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx
IdP	Identity Provider	
NIPG	National Identity Proofing Guidelines	
NISCG	National Identity Security Coordination Group	
OAIC	Office of the Australian Information Commissioner	https://www.oaic.gov.au
PIA	Privacy Impact Assessment	
PKI	Public Key Infrastructure	
TDIF	Trusted Digital Identity Framework	https://www.dta.gov.au/what-we-do/platforms/identity/