Commonwealth Digital Transformation Agency (DTA)

Second Independent Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework (TDIF)

September 2018 (GC527)

[FINAL]

Contact: Galexia
Level 11, 175 Pitt Street, Sydney NSW 2000
ABN: 72 087 459 989
Ph: +61 2 9660 1111
www.galexia.com
Email: dta@galexia.com

Document Control

Client

This document has been written for the Digital Transformation Agency (DTA).

Document Purpose

This document an external and independent Privacy Impact Assessment (PIA) examining the privacy considerations around the Digital Transformation Agency (DTA)'s proposed Trusted Digital Identity Framework (TDIF) as at September 2018.

Document Identification

Document title	DTA TDIF – Second Independent PIA (September 2018)
Document filename	gc527_dta_tdif_mid_2018_pia_v6_201809_final_Acc.docx

Client Details	**Digital Transformation Agency (DTA)** Australian Government www.dta.gov.au
Client Contact	**Jacob Suidgeest** Director, Privacy and Policy, Identity e: jacob.suidgeest@digital.gov.au (UNCLASSIFIED) e: jacob.suidgeest@dta.gov.au (PROTECTED)

Consultant Details

Galexia Contact	**Peter van Dijk** (Managing Director) Galexia Level 11, 175 Pitt St, Sydney NSW 2000, Australia p: +612 9660 1111 m: +61 419 351 374 e: pvd@galexia.com
Galexia Reference	GC527
Project emails	dta@galexia.com (Galexia and DTA)

Copyright

Contents

1. Overview

1.1. Approach and Scope

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

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by the establishment of the TDIF.

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

1. An initial public independent PIA undertaken by Galexia on the overall concept and design of the Trusted Digital Identity Framework (TDIF) and some of its key components (December 2016 <www.dta.gov.au/files/DTA_TDIF_Alpha_Initial_PIA.pdf>);
2. A second independent public PIA on the planned implementation of the Trusted Digital Identity Framework (TDIF) as at September 2018 (**this PIA**); and
3. Individual PIAs for each Identity Provider (IdP) that applies to be accredited under the Trusted Digital Identity Framework (TDIF) (as required)[1]; and
4. Individual PIAs for other accredited TDIF Participants (such as the Identity Exchange, Attribute Providers and Credential Providers) (as required).

This PIA is the second public PIA undertaken in relation to the TDIF. Many issues were the subject of findings and recommendations in the first PIA.

In total, the initial public PIA (December 2016) made 23 recommendations. They have been addressed as follows:

- Accepted and implemented: **18**
- Delegated to the Governance review: **2**
- Discussed further in this current PIA: **3**

This second public PIA builds on work undertaken in the initial PIA and uses the consistent section headings and follow-on recommendation numbering system, ensuring integrity and traceability across a series of public PIAs

This PIA considers compliance with privacy legislation and relevant privacy measures contained in the TDIF documentation. The PIA also briefly considers issues around overall privacy management and governance. The currency of this PIA is as at end of September 2018.

Information contained in this PIA is based on:

- Meetings with the Digital Transformation Agency (DTA), including senior management, technical staff, and policy staff;
- Privacy Round table and Update – held on 29 June 2018;
- Meetings with potential TDIF Participants and external stakeholders (2016-2018);
- Documentation related to the proposal;
- General research and literature review on privacy and identity verification issues; and
- Review of relevant privacy legislation and guidelines.

[1] Some Identity Providers will also manage their own Credentials, and therefore may be both an Identity Provider and a Credential Service Provider. Entities in this situation will only need to conduct one PIA.

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;
- **Governance**
  The PIA considers the proposed governance arrangements for the TDIF system and how those arrangements will support the ongoing protection of privacy once the TDIF and its components are operational including, for example, arrangements to facilitate independent monitoring and oversight of the system.
- **Future work plan**
  This PIA has identified several priority tasks to be included in the DTA future work plan.

1.2. TDIF Overview

The TDIF

> *enables the reuse of credentials and verified identity attributes provided by an Identity Provider across Relying Parties. The verified identity attributes support the registration of an individual at a Relying Party and the credentials enable ongoing access to the digital services provided by the Relying Party.*[2]

The Digital Transformation Agency (DTA) has been funded for one year (from July 2018) to test the TDIF with certain Commonwealth services and to report back to government with the results and proposals for future funding and use.

Implementation of the TDIF can be broadly divided into two stages:

- **Stage 1:** Select Commonwealth entities will undertake beta testing and will, after successful completion of that testing, provide identity services for and between one another.
- **Stage 2:** The TDIF infrastructure will be used to provide identity services to Commonwealth and non-Commonwealth entities (i.e. State, Territory or private sector entities).[3]

The most relevant components of the TDIF (from a privacy perspective) 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).[4]

[2] Core Technical Requirement (working draft), 2018 v 0.01.

[3] The understanding of the scope of non-Commonwealth participation in Stage 2 is evolving as the needs of stakeholders are identified (in particular, the extent of the non-Commonwealth use of the identity services provided through the TDIF) and the functionality and features of the approach are further developed.

[4] Initially one Commonwealth IDP will be established and accredited, but there are no restrictions on additional Commonwealth IDPs joining the TDIF in the future.

1.3. High Level Privacy Impact of the TDIF System Components

Each of the TDIF components raises slightly different privacy issues. The PIA follows the Commonwealth PIA Guidelines, so each section examines compliance against a specific APP (see the summary in Section 3 below). However, it is also useful to examine the *overall* privacy issues facing each TDIF component, as summarised in the following table:

System Component	Compliance Status	Galexia Findings	Galexia Recommendation[5]
Component 1. **Mandatory policies and standards**	**Action required**	The first key component of the TDIF is the development of mandatory standards, policies and agreements for all participants – usually referred to as the Trusted Digital Identity Framework (TDIF) requirements. 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). Participants risk having their TDIF accreditation revoked if their processes and practices fail to meet the standards. The standards include a key section on privacy (the Privacy Requirements, Trusted Digital Identity Framework (TDIF), February 2018, version 1.0). The TDIF Privacy Requirements are likely to have a positive impact on the protection of privacy. However, confidence in the privacy standards would be boosted by some form of legislative backing to ensure that participants are bound to the key privacy standards, and that the standards will not change without public scrutiny.	**R24: The TDIF Privacy Requirements should be strengthened by enshrining them in a legislative instrument** Confidence in the TDIF Privacy Requirements would be boosted by some form of legislative backing to ensure that participants are bound to the key privacy standards, and that the privacy standards will not change without public scrutiny.
Component 2. **The Identity Exchange**	**Action required**	The Identity Exchange includes features that are designed to minimise the amount of personal data that is collected and stored, to 'blind' identity providers 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 are privacy positive. Some concerns remain in relation to the collection, use and disclosure of metadata by the Identity Exchange – as this has a negative impact on key privacy issues (such as function creep and the potential use of TDIF data for surveillance and monitoring). For example, privacy may best be protected by only retaining meta-data on the last 10-20 transactions or for 12-18 months (whichever period is shorter). The exact periods will be the subject of further discussion and evaluation.	**R25: The Identity Exchange should only retain metadata for a short period** The period that meta-data needs to be retained by the Identity Exchange in order to facilitate the investigation of identity fraud and suspicious transactions should be restricted.

[5] Recommendation numbering is continued from the initial TDIF PIA (December 2016) <https://www.dta.gov.au/files/DTA_TDIF_Alpha_Initial_PIA.pdf. Refer to Section 1.6. DTA Privacy Work Plan for assessment of progress against the earlier recommendations.

System Component	Compliance Status	Galexia Findings	Galexia Recommendation[5]
Component 3. **Identity Providers (IdPs)**	**In progress**	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 ATO has been commissioned to develop an IdP. They will need to be accredited against the TDIF requirements. There is no restriction on the development of further Commonwealth IdPs in time.	

1.4. Australian Privacy Principle (APP) Compliance

This PIA assesses the proposed development of the TDIF against the APPs in the Commonwealth *Privacy Act*. Additionally, this PIA recommends privacy protection measures in areas where the APPs do not provide sufficient clarity for a nationally federated digital identity system. This approach is already contemplated in the TDIF by the establishment of the TDIF Privacy Requirements (2018 version 1.0).

For simplicity, this section of the PIA uses the structure and numbering of the APPs to summarise findings and issues. Cross reference to the relevant TDIF Privacy Requirements are also included.

The following table summarises the main findings at this stage of the project:

Australian Privacy Principle (APP)	Indicative Compliance Status	Galexia Findings	Galexia Recommendation
APP 1 – **Open and transparent management**	**Action required**	APP 1 requires all TDIF Participants to be open and transparent about the collection, use and disclosure of data. The OAIC is active on enforcement of APP 1. APP 1 (and its TDIF equivalent – section 2.2.2 of the TDIF Privacy Requirements) require participants to publish a privacy policy containing key information. This requirement should not present major difficulties. However, there may be confusion for consumers if TDIF Participants try to include information on the TDIF in their normal corporate privacy policies. Stand-alone privacy policies for the Identity Exchange and each IdP will deliver significant benefits. For example, the IdP function will be a relatively minor activity within a major agency (such as the ATO) or a large commercial sector IdP (such as a bank). The rules that apply to the IdP activity will be different to the rules that apply to their other day-to-day services. There are numerous precedents in the Australian context. For example, the Australian Bureau of Statistics (ABS) has a general privacy policy for its day-to-day activities and a separate privacy policy for the Census.[6]	**R26: The Identity Exchange and accredited IdPs should develop stand-alone privacy policies** The Identity Exchange and accredited IdPs should be required to develop stand-alone privacy policies that explain the specific collection, use and disclosure of personal information in that role. This should be a TDIF accreditation requirement.

[6] <http://www.abs.gov.au/privacy>

Australian Privacy Principle (APP)	Indicative Compliance Status	Galexia Findings	Galexia Recommendation
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.[7] There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level. Some IdPs may offer to support services at Level 1, and this will facilitate the use of anonymous and pseudonymous services. However, this is not a mandatory TDIF requirement. 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 the focus of the TDIF, and is not the subject of detailed consideration in this PIA.	
APP 3 – Collection of solicited personal information	**Action required**	**Data minimisation** The TDIF Privacy Requirements 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). The TDIF Privacy Requirements also include a specific requirement on data minimisation. They require participants to: *'Only disclose the minimum identity attributes required for the Relying Party's transaction (e.g. supply proof of age rather than date of birth if that is all that is required)'* (Section 2.6). **Biometrics** The initial PIA (2016) included a recommendation (R12) to strengthen the protections for biometric information. This has been actioned by a new set of specific requirements for System participants in the TDIF Privacy Requirements: *'An Applicant MUST only collect sensitive information as defined in the Privacy Act 1988 (including biometric information and biometric templates) with the explicit consent of the individual.* *A biometric collected to verify an individual's attributes (for example matching a person's face to a photo document):* – *MUST NOT be used for any other purpose.* – *MUST NOT be disclosed to a third party.* – *MUST be destroyed once the verification process has concluded.'* (Section 2.7) These restrictions are a key privacy positive feature of the TDIF. However, it is essential that these restrictions are supported by legislation.	**R27: Strengthen the TDIF governance arrangements to ensure that the requirements on biometrics receive suitable legislative backing** The Digital Transformation Agency (DTA) should seek specific legislative backing for the TDIF restrictions on the use of biometrics, namely: 1. The biometrics must not be used for any other purpose; 2. The biometrics must not be disclosed to a third party; and 3. The biometrics must be destroyed once the verification process has concluded.

[7] Refer to the TDIF Identity Proofing Requirements v1.06 (March 2018) <https://www.dta.gov.au/files/identity/tdif-identity-proofing-requirements.pdf>

Australian Privacy Principle (APP)	Indicative Compliance Status	Galexia Findings	Galexia Recommendation
APP 4 – Dealing with unsolicited personal information	**Compliant**	It is difficult to see how unsolicited information might be received by participants in the TDIF when they are engaged in identity related activities. This principle on unsolicited information is not included in the TDIF Privacy Requirements. This issue is not the subject of detailed consideration in this PIA.	
APP 5 – Notification	**Compliant**	Both APP 5 and the TDIF Privacy Requirements (section 2.5) require all accredited participants to provide notice to individuals regarding key aspects of the collection, use and disclosure of their information. Compliance with these provisions is not expected to cause difficulties. Each accredited party (e.g. Identity Providers and Attribute Providers) will confirm compliance with the notice requirements as part of their TDIF accreditation and ongoing audit processes.	
APP 6 – Use or Disclosure	**Compliant**	**Law enforcement access** The Initial PIA (2016) recommended (R13) that the TDIF should publish annual Transparency Reports related to law enforcement access requests. This recommendation has now been implemented through the TDIF Privacy Requirements for the Identity Exchange to: *'publish in an open and accessible manner an annual Transparency Report that discloses the scale, scope and reasons for access to personal information by enforcement bodies.'* (section 2.6.1). **User choice** Stakeholders have expressed concern over whether the use of the TDIF is voluntary or mandatory. The TDIF is designed to be voluntary, but an appropriate level of user choice may be difficult to implement in practice. The TDIF Privacy Requirements require participants to explain user choices: *'The Applicant MUST inform users of other channels available to verify identity and make clear to the user what the consequences are of declining to provide the required information'* (section 2.8). However, the requirement to explain user choice is not the same as a requirement to always offer user choice. This issue is discussed in further detail in the section below on privacy management and governance.	
APP 7 – Direct Marketing	**Compliant**	The initial PIA (2016) recommended (R14) that the use of TDIF data for direct marketing should be prohibited. The use of personal data for direct marketing is now completely prohibited in the TDIF Privacy Requirements (section 2.6).	

Australian Privacy Principle (APP)	Indicative Compliance Status	Galexia Findings	Galexia Recommendation
APP 8 – Cross Border Disclosure	**Compliant**	The Initial PIA (2016) recommended (R16) that the TDIF should insist on a single approach to protecting privacy in the case of cross border data transfers. It did not recommend a complete prohibition on cross-border data transfers. The TDIF Privacy Requirements now contain a stand-alone cross border data transfer requirement that extends the requirements to all 'contractors' even if the data is retained in Australia. The TDIF includes a prohibition on the use of the data by recipients such as cloud service providers for any purpose other than identity verification, and also includes some specific requirements relating to enforceable contracts and audits (section 2.9). These requirements are considerably broader and stronger than APP 8, and provide a suitable level of privacy protection.	
APP 9 – Government Related Identifiers	**Compliant**	APP 9 does not provide a sufficient level of privacy protection in relation to the potential use of identifiers in the TDIF, especially as Commonwealth Agencies are exempt from APP 9 (and this is likely to include the Identity Exchange and at least one Commonwealth IdP). This was considered in the Initial PIA (2016) and specifically in recommendations R17 and R18. The TDIF Privacy Requirements now include a provision on identifiers that can be applied to all participants: *'An Applicant MUST NOT create a new government identifier that is used across the identity federation (ie an identifier that is sent to more than one Relying Party or Identity Service Provider)'* (section 2.10) This prohibition represents a significant strengthening of the privacy protection measures in the TDIF.	
APP 10 – Quality of Personal Information	**Action Required**	**Finding:** The current TDIF design includes a range of measures to ensure data quality. Ensuring data quality is also included in the TDIF Privacy Requirements (section 2.12) and include specific training and audit requirements in relation to data quality at IdPs (section 2.12.1). However, an important part of APP 10 is that information should be *'up to date having regard to the purpose of the use or disclosure'*. At the time of preparing this PIA, the time periods for validity and renewal of identities have not been confirmed. It will be difficult to ensure compliance with APP 10 until this issue is addressed.	**R28: Establish a time period for the validity and renewal of identity credentials** The TDIF should include a specific requirement and process for the renewal of identity credentials to ensure that information is 'up to date having regard to the purpose of the use or disclosure' of the identity information.

Australian Privacy Principle (APP)	Indicative Compliance Status	Galexia Findings	Galexia Recommendation
APP 11 – Security	**In Progress**	The data being exchanged in the TDIF includes sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches. APP 11 provides a very high level requirement that security measures are proportionate to the risk of a security breach. APP 11 is supplemented by more detailed security requirements in the TDIF accreditation process. The TDIF accreditation model is a good mechanism for ensuring consistent and appropriate security measures are in place across the entire TDIF. The requirements in the three documents set out above are much more specific than APP 11. As all TDIF applicants will be separately accredited against these higher security standards, specific security measures are not considered in detail in this PIA.	
APP 12 – Access	**Compliant**	The Initial PIA (2016) recommended (R19) that the Identity Exchange should be required to provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transactions or identity fraud. The TDIF Privacy Requirements now include this provision: *'The Identity Exchange MUST provide individuals with access to the metadata on transactions it logs (ie that has not been deleted under its destruction policy) in a dashboard format.* *Note: An Identity Exchange will not be able to directly identify an individual and therefore the individual will need to access its metadata by logging on through an Identity Service Provider'* (section 2.11.3).	
APP 13 – Correction	**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 Initial PIA (2016) made several recommendations (R22 and R23) to improve complaints handling processes. The TDIF Privacy Requirements now include a detailed complaints process. One important requirement is that each Participant's complaints process must be: *'integrated with other complaint handling bodies, (e.g other participants of the identity federation) so it can assist the user and refer complaints'* (section 2.13). One minor outstanding issue is that all TDIF applicants should be required to respond to complaint and requests to correct data within 30 days.	**R29: Ensure a consistent timeframe for responding to complaints and correcting data** In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints and to address request to correct data within 30 days

1.5. Governance Arrangements

The DTA is developing legal and governance arrangements for the TDIF system to address compliance, liability and legal effectiveness considerations. These arrangements will underpin key privacy aspects of the TDIF including the double-blind as the key privacy-by-design feature.

To support a 'live' system, it is necessary to have:

- Comprehensive contractual arrangements between participants ("Operating Rules"); and
- An "Oversight Authority" who will regulate and enforce these arrangements (in line with the double-blind privacy requirements of the system).

This PIA has also considered how ongoing governance arrangements can be strengthened to protect against system changes or 'function creep' that may erode privacy protections over time.

R30: Consumer and community representation in oversight of the TDIF
Key stakeholder representatives (from government, community and business) should be provided with an appropriate mechanism to formally participate in the development and implementation of the TDIF. This could take the form of an advisory committee – to be consulted by the Oversight Authority as appropriate.

R31: Mandatory review of TDIF after three years
The entire TDIF design, implementation and experience should be the subject of a major review after three years, to assess the effectiveness of privacy protections and to guard against any divergence from the original TDIF objectives and privacy promises.

Further consideration of governance is set out in Section 19.

1.6. DTA Privacy Work Plan

This PIA has made a range of recommendations to address privacy concerns. Some 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. The table also includes *previous* recommendations made in the initial PIA[8], many of which have been implemented:

Component / APP	Recommendation	Action Required	Person / Agency responsible	Status / Timing
Initial PIA (December 2016)				
Component 1. **Mandatory policies and standards**	**R1:** The TDIF accreditation / revocation proposal	Clarify and explain the detailed powers behind this proposal	DTA	Delegated to the Governance Review
	R2: Privacy principles in the Core Service Requirements	Develop a set of draft Privacy Principles and consult with stakeholders	DTA	Implemented
Component 2. **The Identity Exchange**	**R3:** The Identity Exchange and the retention of metadata	Determine a specific meta-data retention period	DTA	Discussed further in this PIA (2018). Refer to R25.
Component 3. **Identity Providers (IdPs)**	**R4:** The selection of a single Commonwealth IdP – further consultation	Further stakeholder engagement (workshop / consultation)	DTA	Implemented
	R5: The selection of a single Commonwealth IdP – risk assessment	Completion of a detailed risk assessment	Independent provider	Implemented
Is the data 'personal information'?	**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	Implemented
	R7: The Identity Exchange and the definition of Personal Information	The Identity Exchange documentation should classify all data as personal information.	DTA	Implemented
APP 1 – **Open and transparent management**	**R8:** Openness Task	The Identity Exchange should develop a specific privacy policy	DTA	Implemented
APP 3 – **Collection of solicited personal information**	**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	Implemented
APP 5 – **Notification**	**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	Implemented
APP 6 – **Use or Disclosure**	**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	Discussed further in this PIA (2018). Refer to R25.

[8] Refer to Initial public independent PIA undertaken by Galexia on the overall concept and design of the Trusted Digital Identity Framework (TDIF) and some of its key components (December 2016 <www.dta.gov.au/files/DTA_TDIF_Alpha_Initial_PIA.pdf>.

Component / APP	Recommendation	Action Required	Person / Agency responsible	Status / Timing
	R12: Use of biometric data	The TDIF Core Service Requirements should incorporate some additional privacy protections for the use of biometric data.	DTA	Implemented
	R13: Development of a transparency report	The TDIF should publish an annual transparency report on law enforcement access.	DTA	Implemented
APP 7 – Direct Marketing	**R14:** Direct marketing prohibition	The use of TDIF personal data for direct marketing should be prohibited in the TDIF Core Service Requirements	DTA	Implemented
APP 8 – Cross Border Disclosure	**R15:** Cross border data transfer – mapping	Each TDIF participant should identify and map their cross-border data transfers.	DTA / IdPs	Implemented
	R16: Cross border data transfer – protection	The TDIF Core Service Requirements should include stronger and more consistent principles on cross border disclosures.	DTA	Implemented
APP 9 – Government Related Identifiers	**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	Implemented
	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	Implemented
APP 10 – Quality of Personal Information	**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	Implemented
	R20: Access requests – consistency	The TDIF Core Service Requirements should adopt common access requirement across all IdPs.	DTA	Implemented
APP 13 – Correction	**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	Implemented
	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	Discussed further in this PIA (2018). Refer to R29.
Governance	**R23:** Governance arrangements	The DTA has recently commissioned work on governance arrangements for the TDIF. This work should consider the governance issues raised in the initial PIA.	Independent provider	Delegated to the Governance Review
This PIA (September 2018)				
Component 1. Mandatory policies and standards	**R24:** Legislation	The TDIF Privacy Requirements should be strengthened by enshrining them in a legislative instrument	DTA	Refer to Appendix – DTA Response
Component 2. The Identity Exchange	**R25:** Retention of meta-data	The Identity Exchange should only retain metadata for a short period	DTA / Identity Exchange	

Component / APP	Recommendation	Action Required	Person / Agency responsible	Status / Timing
APP 1 – Open and transparent management	**R26:** Openness	The Identity Exchange and accredited IdPs should develop stand-alone privacy policies	DTA / Participants	
APP 3 – Collection of solicited personal information	**R27:** Biometrics	Strengthen the TDIF governance arrangements to ensure that the requirements on biometrics receive suitable legislative backing	DTA	
APP 10 – Quality of Personal Information	**R28:** Data quality	Establish a time period for the validity and renewal of identity credentials	DTA	
APP 13 – Correction	**R29:** Complaints	Ensure a consistent timeframe for responding to complaints and correcting data	DTA	
Governance	**R30:** Consumer and community representation in oversight of the TDIF	Key stakeholder representatives should be provided with an appropriate mechanism to participate in the oversight of the TDIF.	DTA	
	R31: Mandatory review of TDIF after three years	The entire TDIF design, implementation and experience should be the subject of a major review after three years.	DTA	

2. TDIF – System Overview

2.1. High Level Description

The Digital Transformation Agency (DTA) has policy responsibility for the establishment of a Trusted Digital Identity Framework (the TDIF).

Delivery and use of the TDIF can be broadly divided into two stages:

- **Stage 1:** Select Commonwealth entities will undertake beta testing and will, after successful completion of that testing, provide identity services for and between one another.
- **Stage 2:** The TDIF infrastructure will be used to provide identity services to Commonwealth and non-Commonwealth entities (i.e. State, Territory or private sector entities).[9]

The DTA has been funded for one year to test the TDIF with certain Commonwealth services and to report back to government with the results and proposals for future funding and use.

The TDIF:

> *enables the reuse of credentials and verified identity attributes provided by an Identity Provider across Relying Parties. The verified identity attributes support the registration of an individual at a Relying Party and the credentials enable ongoing access to the digital services provided by the Relying Party.*[10]

The most relevant components of the TDIF (from a privacy perspective) are:

1. The proposed development of mandatory standards, policies and agreements for all System participants;
2. The proposed development of an Identity Exchange; and
3. The proposed development of a Commonwealth Identity Provider (IdP).[11]

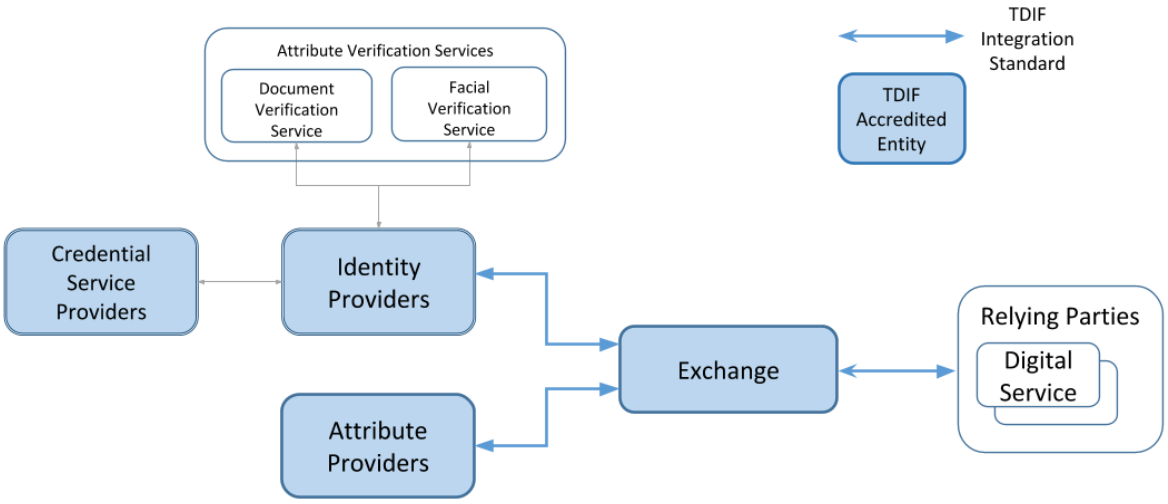

Figure 1: TDIF Overview (Source: DTA, August 2018)

[9] The understanding of the scope of non-Commonwealth participation in Stage 2 is evolving as the needs of stakeholders are identified (in particular, the extent of the non-Commonwealth use of the identity services provided through the TDIF) and the functionality and features of the TDIF are further developed.

[10] Core Technical Requirements (working draft), 2018 v0.01.

[11] Initially one Commonwealth IDP will be established and accredited, but there are no restrictions on additional Commonwealth IDPs joining the TDIF in the future.

2.2. Component 1: Policies and standards

The first key component of the TDIF is the proposed development of mandatory standards, policies and agreements for all participants. Refer to Appendix – TDIF Policies and Standards

Compliance with these standards will be mandatory – each 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.

2.3. Component 2: The Identity Exchange

An important component of the TDIF is the proposed Identity Exchange. 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 digital identity 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).

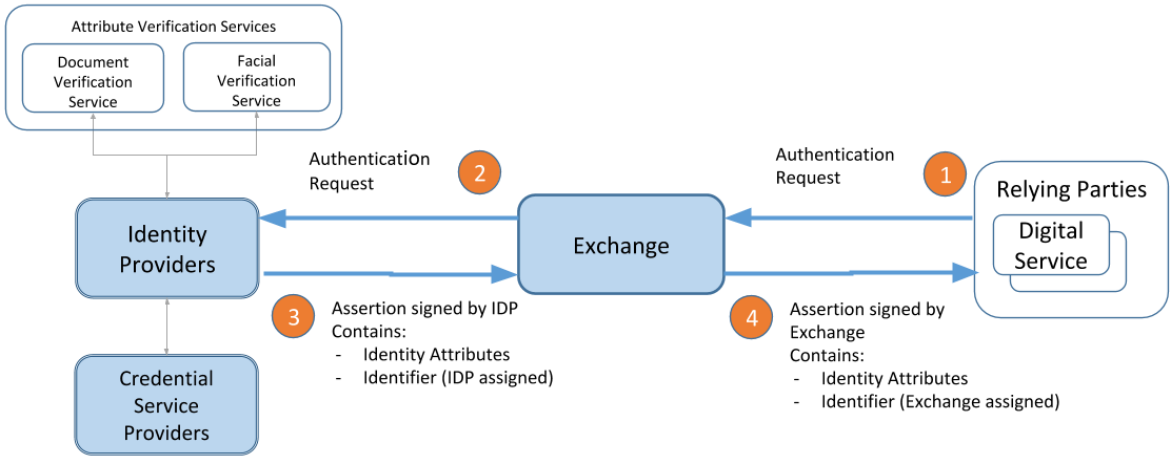

Figure 2: The Role of the Identity Exchange (Source: DTA, August 2018)

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.

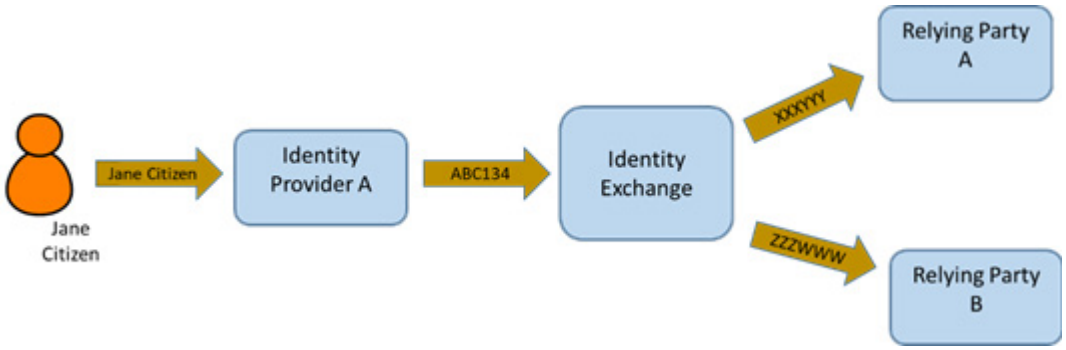

Figure 3: Blinding by the Identity Exchange (Source: DTA, August 2018)

The Identity Exchange is not designed to become a central repository of identity data, and IdPs do not obtain logs of the services being used by their customers. The privacy objective is to ensure that identity providers don't have access to an individual's service access over time so the information cannot be used to commercialise the data or to profile individuals. 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; 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.

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.

These issues are the subject of further discussion in this PIA.

2.4. 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.

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 eventually operate 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.

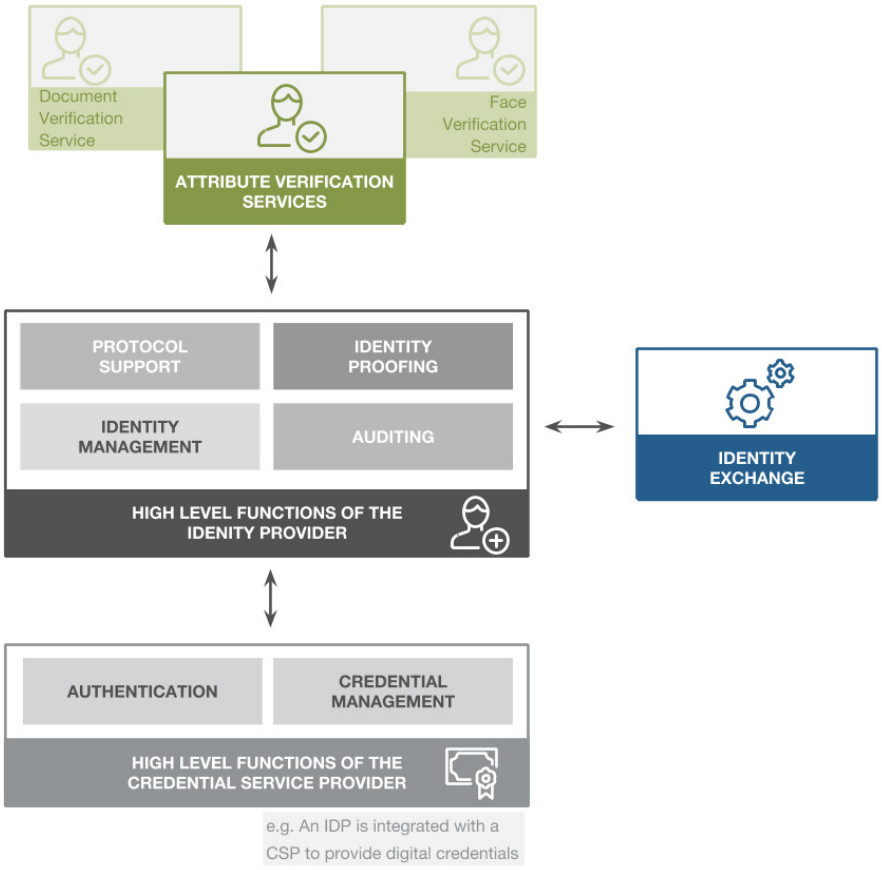

Figure 4: Identity Providers (Source: DTA, August 2018)

2.5. Other TDIF System Components

Other components of the TDIF system include:

- **Relying Parties**
  Relying Parties are the organisations or government agencies that rely on verified attributes or assertions provided by an Applicant through an Identity Exchange to enable the provision of a digital service. Relying Parties are the organisational entities that provide digital services and will be approved to use the system.

- **Attribute Providers**
  The Exchange may mediate interactions with additional Attribute Providers to support the sharing of attributes that are in addition to the core identity attributes available for individuals from Identity Providers. An Attribute Provider needs to be an authoritative source of attributes and must be accredited. Typically, an Attribute Provider will be integrated with a registry that holds the attributes (for example: the Australian Health Practitioner Regulation Agency (AHPRA)).

- **Credential Service Providers**
  Credential Providers generate and manage authentication credentials which are provided to people. This function may be internalised within an IdP. Each Credential Service Provider must be accredited.

- **Attribute Verification Services**
  Attribute Verification Services enable the verification of attributes against the authoritative source. Attributes that are based on identity documents can be verified using the Document Verification Service (DVS). For documents that include a biometric image of a person, i.e. a photo ID, the Face Verification Service (FVS) can be used to achieve a higher level of assurance in the identity verification process,

2.6. Information Flows

The key information flow is the identity linking process, as shown in the following diagram:

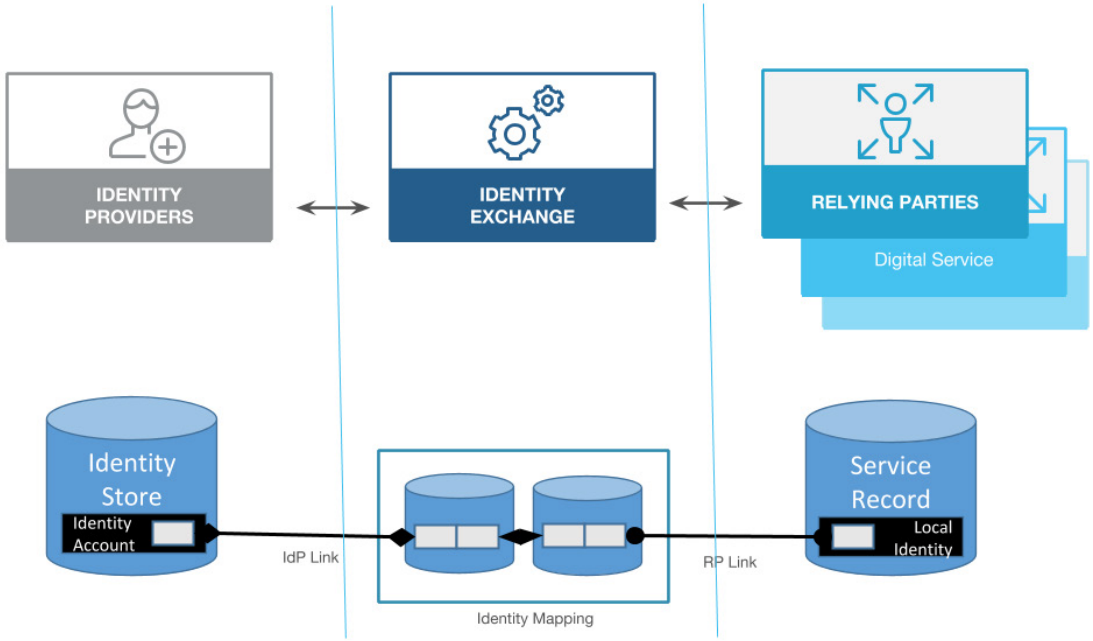

Figure 5: Identity linking (Source: DTA, August 2018)

The identity links in the TDIF are used to support the authentication processes that enable an individual to have ongoing access to digital services at a Relying Party. The authentication process for an individual at a Relying Party typically includes two key steps as follows:

1. **Establishing a local identity at the Relying Party.**
   An individual has verified identity attributes at an Identity Provider. The individual authenticates at an Identity Provider and consents to the release of these verified identity attributes (and possibly additional attributes) to the Relying Party via the Identity Exchange. The Relying Party then uses the identity attributes to identify any existing service record they may hold for the individual by performing Identity Matching. If no existing identity record is found, the Relying Party creates a service record for the user. If continued access to digital services is required, the Relying Party stores the RP Link provided by the Identity Exchange.
2. **Accessing digital services at the Relying Party.**
   Once the service record at a Relying Party has been established the user can access digital services by authenticating at the Identity Provider via the Identity Exchange.

2.7. Pilots

In late 2018 the Government will begin rolling out opt-in digital identity pilots with high volume government services. The proposed Pilots include:

1. **Tax file number**
   The first service to accept digital proof of identity is the Australian Taxation Office's new tax file number registration system. Around 775,000 applications for a tax file number are made every year. This pilot will allow a sample group of individuals to apply for a Tax File Number using a digital identity.
2. **Australian Business Registry**
   The Australian Business Registry stores details about businesses and organisations that have an Australian Business Number (ABN). Around 160,000 individuals access the Australian Business Registry annually on behalf of a business. This pilot will allow a sample group of individuals to access the Australian Business Registry using a digital identity.
3. **Grant management**
   Up to 5,000 organisations regularly manage, report and acquit government grants. This pilot will allow selected organisations and individuals to access online grant systems using a digital identity.
4. **Unique Student Identifier**
   A Unique Student Identifier is an identification number people need when completing any nationally recognised training. A Unique Student Identifier gives a student an online record of all their training and qualifications. This pilot will examine options for obtaining a Unique Student Identifier using a digital identity.
5. **Centrelink online accounts**
   The Centrelink Online Account will allow people to access Centrelink services online without first having to present at a government service centre. There are 432,000 new Centrelink customers annually, the majority of which are jobseekers or students. The creation of a Centrelink Online Account through digital identity will also support the Youth Allowance and Newstart Allowance pilot services outlined below.
6. **Youth Allowance**
   Each year 200,000 enrolments in Youth Allowance support young Australian students and jobseekers. This pilot will make it possible for a sample group of young Australians to access this support in 2018–19.
7. **Newstart Allowance**
   Newstart Allowance allows 790,000 jobseekers annually to access support, with only 38% able to access these services online. This pilot will make it possible for a sample group of individuals to access services online.
8. **My Health Record**
   The My Health Record initiative will see 25 million online health records being created. This pilot program will allow a sample group of individuals to use their digital identity to create their My Health Record account online.

3. Governance

The TDIF is a complex program involving a range of stakeholders from government (including Commonwealth, State and Territory), community and the private sector. As noted above, legal and governance arrangements for the TDIF are therefore necessary to address issues relating to compliance, liability and legal effectiveness.

3.1. Oversight of the TDIF system

The legal and governance arrangements for the TDIF system will be administered and enforced by an Oversight Authority. The Oversight Authority will be the organisation empowered to address breaches of the system by participants (and related issues) and, where appropriate, override the 'double-blind' system requirements to ensure the system operates effectively. For this reason, the Oversight Authority must be independent (i.e. not have any conflicting roles in the system).

The Oversight Authority will:

- administer, enforce and maintain the TDIF;
- accredit or approve participants in the system;
- deal with participants if accreditation or approval requirements are not maintained;
- manage complaints and public enquiries;
- conduct investigations (e.g. fraud);
- monitor compliance with the TDIF;
- enforce service levels (as applicable); and
- manage fees and charges (as applicable).

As noted above, parties who wish to participate in the TDIF system will need to satisfy a range of criteria and requirements set out in the TDIF. Participants will need to be accredited or approved against these criteria and requirements upon initial application, and on an ongoing basis.

The following chart shows the TDIF components that will require accreditation:

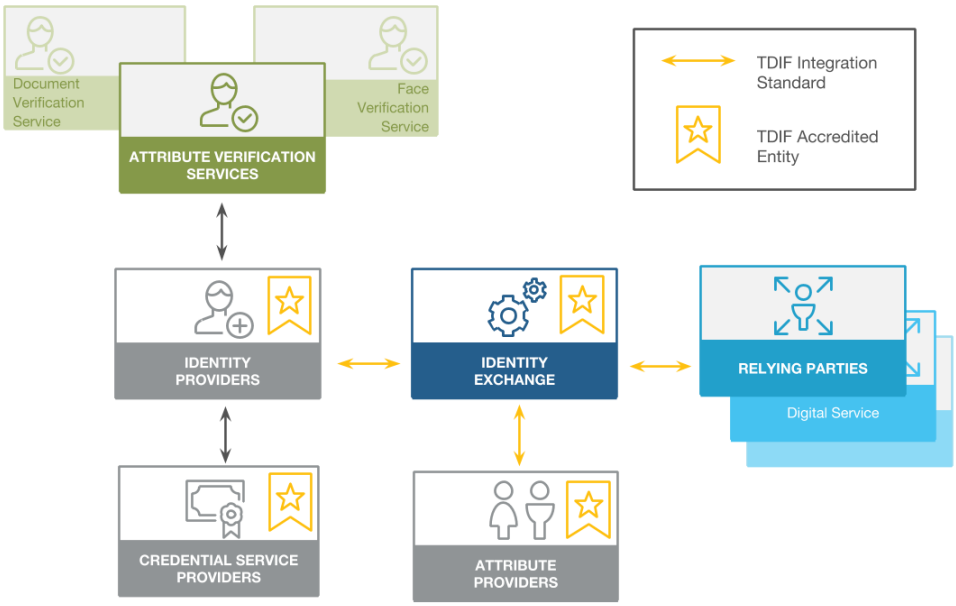

Figure 6: Accreditation (Source: DTA, August 2018)

The DTA is currently exploring options for the Oversight Authority (including interim and end-state options).

3.2. Operating Rules

The Oversight Authority will regulate and enforce comprehensive binding arrangements between participants – the "Operating Rules". The Operating Rules will incorporate and build on current TDIF requirements and will be structured to give certainty to system participants about their roles and responsibilities within the system. Participants could be contractually bound to comply with the Operating Rules. Alternatively, legislation could set out the Operating Rules (or provide a mechanism through which the Operating Rules are established – e.g. legislative instrument).

The DTA is currently considering options for the development of binding arrangements for the TDIF system.

4. High Level Privacy Impact of the TDIF System Components

Each of the TDIF components raises slightly different privacy issues. It is useful to examine the *overall* privacy issues facing each TDIF component.

4.1. Component 1. Mandatory Policies and Standards

The first key component of the TDIF is the development of mandatory standards, policies and agreements for all participants – usually referred to as the Trusted Digital Identity Framework (TDIF) Requirements. Refer to Appendix – TDIF Policies and Standards.

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). Participants risk having their TDIF accreditation revoked if their processes and practices fail to meet the standards.

The standards include a key section on privacy (the Privacy Requirements, Trusted Digital Identity Framework (TDIF), February 2018, version 1.0 <www.dta.gov.au/files/identity/tdif-privacy-requirements.pdf>). Stakeholders have had opportunities to comment on the draft standards.

The TDIF Privacy Requirements are likely to have a positive impact on the protection of privacy. However, confidence in the standards would be boosted by some form of legislative backing to ensure that TDIF Participants are bound to the key privacy standards, and that the standards will not change without public scrutiny.

The key TDIF Privacy Requirements that must be enshrined in legislation are:

1. The structural separation and independence of the Identity Exchange;
2. The prohibition on the use of TDIF data for direct marketing
3. The prohibition on the use of identity data (e.g. by contractors) for any purpose other than identity verification;
4. The restrictions on the use of biometrics (see also the discussion at APP 3 Collection and Recommendation 27); and
5. The restrictions on the use of identifiers.

Recommendation 24: The TDIF Privacy Requirements should be strengthened by enshrining them in a legislative instrument
Confidence in the TDIF Privacy Requirements would be boosted by some form of legislative backing to ensure that participants are bound to the key privacy standards, and that the privacy standards will not change without public scrutiny.

4.2. Component 2. The Identity Exchange

The Identity Exchange includes features that are designed to minimise the amount of personal data that is collected and stored, to 'blind' identity providers 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 are privacy positive.

Some concerns remain in relation to the collection, use and disclosure of metadata by the Identity Exchange – as this has a negative impact on key privacy issues (such as function creep and the potential use of TDIF data for surveillance and monitoring).

For example, privacy may best be protected by only retaining meta-data on the last 10-20 transactions or for 12-18 months (whichever period is shorter). The exact period will be the subject of further discussion and evaluation.

Recommendation 25: The Identity Exchange should only retain metadata for a short period
The period that meta-data needs to be retained by the Identity Exchange in order to facilitate the investigation of identity fraud and suspicious transactions should be restricted.

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 ATO has been commissioned to develop an IdP. They will need to be accredited against the TDIF requirements.

There is no restriction on the development of further Commonwealth IdPs in time.

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.*
> <www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#personal-information>

5.2. OAIC Guidelines

In May 2017 the OAIC provided guidance on personal information:

> *What Is Personal Information?,* Office of the Australian Information Commissioner (OAIC), 5 May 2017 <https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>.

This provides 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.*

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.*

5.3. 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. 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	Mandatory for verification and authentication	Stored permanently by the IdP
Date of birth	Yes	Collected at enrolment	Mandatory for verification and authentication	Stored permanently by the IdP
Address	Yes	May be collected at enrolment	Address data is not verified, but the 'asserted' address is an attribute that may be shared under the TDIF with the customer's consent.	Stored permanently by the IdP
Email address	Yes	May be collected at enrolment	May be used for sending security tokens and other limited purposes.	Stored permanently by the IdP
Mobile phone number	Yes	May be collected at enrolment	May be used for sending security tokens and other limited purposes.	Stored permanently by the IdP
Face image / photograph / biometric template	Yes	Collected at enrolment but immediately deleted following the FVS check.	Mandatory for verification at enrolment. Prohibited for any other use.	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.	Mandatory for verification at enrolment	Checked against the Document Verification Service (one time only). Copies of documents and / or document references may be retained by the IdP Some form of transaction record / receipt maintained to provide assurance that the match with DVS was undertaken.

There will be 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). The Identity Proofing Requirements preclude an individual having multiple identities in the one IDP or in different IDPs. Individuals may have multiple credentials associated with that identity (e.g. credentials for multiple devices or replacement credentials for earlier / lost credentials .[12] (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 across the entire Federation. It is just used within the IdP and in interactions between the IdP and the Identity Exchange. Relying Parties, for example, do not see this unique number. 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.

5.4. 'Personal information' Finding

The Privacy Commissioner advises 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*[13]

In the case of the TDIF this PIA treats all data collected, stored and used by Identity Providers (IdPs) as Personal Information under the Privacy Act.

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

[13] Office of the Australian Information Commissioner (OAIC), Guide to securing personal information, 2015, <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-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: <www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

6.2. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs. The APP 1 'equivalent' in the TDIF Privacy Requirements is *Section 2.2.2. Polices,* although some other sections also covers broader issues of openness (such as the sections on privacy governance).

Section 2.2.2 of the TDIF Privacy Requirements requires participants to publish a privacy policy containing key information. This will need to be applied to IdPs, the Identity Exchange and other accredited parties, such as Attribute Providers.

The following checklist provides a useful summary of the key issues regarding openness and transparency:

APP1. Openness and Transparency of Management of Personal Information	Action / Status	Galexia Commentary
A. Does the entity provide a public privacy policy?	**Action Required**	APP 1 requires all TDIF Participants to be open and transparent about the collection, use and disclosure of data. The OAIC is very active on enforcing APP 1 APP 1 (and its TDIF equivalent – section 2.2.2 of the TDIF Privacy Requirements) require participants to publish a privacy policy containing key information. This requirement should not present major difficulties. However, there may be confusion for consumers if TDIF Participants try to include information on the TDIF in their normal corporate privacy policies. Stand-alone privacy policies for the Identity Exchange and each IdP will deliver significant benefits. For example, the IdP function will be a relatively minor activity within a major agency (such as the ATO) or a large commercial sector IdP (such as a bank). The rules that apply to the IdP activity will be different to the rules that apply to their other day-to-day services. There are numerous precedents in the Australian context. For example, the Australian Bureau of Statistics (ABS) has a general privacy policy for its day-to-day activities and a separate privacy policy for the Census.[14] **Recommendation 26: The Identity Exchange and accredited IdPs should develop stand-alone privacy policies** The Identity Exchange and accredited IdPs should be required to develop stand-alone privacy policies that explain the specific collection, use and disclosure of personal information in that role. This should be a TDIF accreditation requirement.
B. Does the Policy include: (a) the kinds of personal information that the entity collects and holds;	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
C. Does the Policy include: (b) how the entity collects and holds personal information;	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
D. Does the Policy include: (c) the purposes for which the entity collects, holds, uses and discloses personal information;	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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;	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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;	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.

[14] <www.abs.gov.au/privacy>

APP1. Openness and Transparency of Management of Personal Information	Action / Status	Galexia Commentary
G. Does the Policy include: (f) whether the entity is likely to disclose personal information to overseas recipients;	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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.	**Compliant**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.

6.3. APP 1. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.2.2 Policies*. The requirements in this section are closely aligned to APP 1 and provide a suitable level of privacy protection.

This PIA recommends that the Identity Exchange and accredited IdPs should be required to develop stand-alone privacy policies that explain the specific collection, use and disclosure of personal information in that role. (refer to Recommendation 26).

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

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

7.2. TDIF – Overview

The prototypes the DTA and its federation partners are building are designed to cater for transactions that require Level 2 and Level 3 identity.[15] There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level.

Some IdPs may offer to support services at Level 1 in the future, and this will facilitate the use of anonymous and pseudonymous services. However, this is not a mandatory TDIF requirement.

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 the focus of the initial prototypes, and is not the subject of detailed consideration in this PIA.

[15] TDIF Identity Proofing Requirements v1.06 (March 2018) <https://www.dta.gov.au/files/identity/tdif-identity-proofing-requirements.pdf>.

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[16] 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

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

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

8.3. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs. The APP 3 'equivalent' in the TDIF Privacy Requirements is *Section 2.6 Collection and use limitation*.

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 general approach to data collection in the TDIF is compliant with APP 3. However, the approach to the collection of biometric data requires further review.

The TDIF Privacy Requirements contain three key restrictions on the use of biometrics, namely:

1. The biometrics must not be used for any other purpose;
2. The biometrics must not be disclosed to a third party; and
3. The biometrics must be destroyed once the verification process has concluded.

These restrictions are a key privacy positive feature of the TDIF.

However, an important function of PIAs is to provide advice on privacy perception issues. Overall, this PIA considers that the lack of legislative backing for the restrictions on biometrics is a potential weakness in the governance arrangements for TDIF.

The TDIF trials are proceeding during a period when the Government is proposing a significant expansion of the use of biometrics (including the expansion of the national biometric capability and the implementation of the Intergovernmental Agreement on Identity Matching Services[17]) for law enforcement and surveillance purposes, and although the TDIF is not included in this expanded use, it is likely that some confusion between the two issues may occur in the eyes of the community.

These perception issues are not assisted by the fact that TDIF will use the same agreements, processes and underlying infrastructure that Agencies use for the surveillance and law enforcement access to biometrics.

[17] https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf

The key TDIF restrictions on the use of biometrics are not set out anywhere in legislation, they are only contained in the TDIF accreditation requirements, which are policy documents that can be changed at any time.

In addition, the *Privacy Act* does not provide backstop privacy protection for the restricted use of biometrics, as it includes significant exemptions related to national security, law enforcement and safety. Similarly, the *Identity-matching Services Bill* 2018 (not yet enacted) does not provide backstop privacy protection, as it also includes significant exemptions related to legal authority, national security and the safety of individuals.

The following table summarises progress against the requirements of APP 3, with a particular emphasis on privacy perception issues and potential community concerns:

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?	**Compliant**	**Data minimisation** The TDIF Privacy Requirements 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). The Privacy Requirements also include a specific requirement on data minimisation. They require participants to: *'Only disclose the minimum identity attributes required for the Relying Party's transaction (e.g. supply proof of age rather than date of birth if that is all that is required)'* (Section 2.6).
B. Is NO sensitive information about an individual collected (unless a relevant exception applies, such as the receipt or explicit and specific consent)?	**Action Required**	**Biometrics** The only sensitive information collected at enrolment in the TDIF is biometric information. The initial PIA (2016) included a recommendation (R12) to strengthen the protections for biometric information. This has been actioned by a new set of specific requirements for System participants in the TDIF Privacy Requirements: *'An Applicant MUST only collect sensitive information as defined in the Privacy Act 1988 (including biometric information and biometric templates) with the explicit consent of the individual.* *A biometric collected to verify an individual's attributes (for example matching a person's face to a photo document):* – *MUST NOT be used for any other purpose.* – *MUST NOT be disclosed to a third party.* – *MUST be destroyed once the verification process has concluded.'* (Section 2.7) These restrictions are a key privacy positive feature of the TDIF. However, it is essential that these restrictions are supported by legislation. **Recommendation 27: Strengthen the TDIF governance arrangements to ensure that the requirements on biometrics receive suitable legislative backing** The Digital Transformation Agency (DTA) should seek specific legislative backing for the TDIF restrictions on the use of biometrics, namely: 1. The biometrics must not be used for any other purpose; 2. The biometrics must not be disclosed to a third party; and 3. The biometrics must be destroyed once the verification process has concluded.
C. Is personal information collected only by lawful and fair means?	**Compliant**	Section 2.6 of the TDIF Privacy requirements requires participants to only collect information by lawful and fair means. IdPs and the Identity Exchange will need to meet this requirement. This will be assessed in the PIAs for individual participants.

APP3. Collection of solicited information	Action / Status	Galexia Commentary
D. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	**Compliant**	Section 2.6 of the TDIF Privacy requirements requires participants to only collect information from the individual, unless it is unreasonable or impractical to do so. IdPs and the Identity Exchange will need to meet this requirement. This will be assessed in the PIAs for individual participants.

8.4. APP 3. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.6 Collection and use limitation*. These requirements are stronger than APP 3 and provide a suitable level of privacy protection.

Two key areas where the collection requirements have been strengthened are the inclusion of a prominent data minimisation requirements and stricter rules for the collection and use of biometrics. These restrictions on the use of biometrics are a key privacy positive feature of the TDIF. However, this PIA has found it is essential that these restrictions are supported by legislation (refer to Recommendation 27).

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

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: <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

This principle on unsolicited information is not usually included in other privacy laws – it is unique to the Commonwealth APPs. It is not included in the TDIF Privacy Requirements, although it will continue to apply to those TDIF Participants who are also subject to the APPs. This will include the Identity Exchange and any Commonwealth Agencies who participate in the TDIF.

This issue is not the subject of detailed consideration in this PIA.

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: <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

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs. The APP 5 'equivalent' in the TDIF Privacy Requirements is *Section 2.5 Notice of collection*.

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?	**Compliant**	Both APP 5 and the TDIF Privacy Requirements (section 2.5) require all accredited participants to provide notice to individuals regarding key aspects of the collection, use and disclosure of their information. 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. Compliance with these provisions is not expected to cause any difficulties. Each accredited party (e.g. Identity Providers and Attribute Providers) will confirm compliance with the notice requirements as part of their TDIF accreditation and ongoing audit processes.

APP 5. Notification	Action / Status	Galexia Commentary
B. Does the entity provide notice of third party collection? (if relevant)	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
D. Does the entity provide notice of the purpose of collection?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.

10.3. APP 5. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.5 Notice of collection*. The requirements in this section are a mirror of APP 5 and provide a suitable level of privacy protection.

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

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.[18]

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

[18] Note: The OAIC have not yet developed the guidelines envisaged under APP 6.3.

11.3. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs. The APP 6 'equivalent' in the TDIF Privacy Requirements is *Section 2.6. Collection and use limitation* and partly *Section 2.8. Consent.*

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.

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

APP 6. Use or Disclosure	Action / Status	Galexia Commentary
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	**Compliant**	**Law enforcement access** The Initial PIA (2016) recommended (R13) that the TDIF should publish annual Transparency Reports related to law enforcement access requests. This recommendation has now been implemented through the TDIF Privacy Requirements for the Identity Exchange to: *'publish in an open and accessible manner an annual Transparency Report that discloses the scale, scope and reasons for access to personal information by enforcement bodies.'* (section 2.6.1). **User choice** Stakeholders have expressed concern over whether the use of the TDIF is voluntary or mandatory. The TDIF is designed to be voluntary, but an appropriate level of user choice may be difficult to implement in practice. The TDIF Privacy Requirements require participants to explain user choices: *'The Applicant MUST inform users of other channels available to verify identity and make clear to the user what the consequences are of declining to provide the required information'* (section 2.8). However, the requirement to explain user choice is not the same as a requirement to always offer user choice. This issue is discussed in further detail in the section below on privacy management and governance.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)?	**Compliant**	Section 2.6 of the TDIF Privacy Requirements states that: *'Excluding uses and disclosures relating to identity verification, which requires consent, and direct marketing, which is prohibited, other uses and disclosures MUST comply with the APPs'* The result of this provision is that secondary use will have to fall within the relevant exceptions in APP 6.

APP 6. Use or Disclosure	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?	**Compliant**	In the TDIF biometric information is only disclosed for the primary purpose and is then immediately destroyed. There is no secondary use of biometric information. See Section 2.7 of the TDIF Privacy Requirements.
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.

11.4. APP 6. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.6 Collection and use limitation* and also partly in *Section 2.8. Consent*. These requirements are stronger than APP 6 and provide a suitable level of privacy protection.

Two key areas where the use and disclosure requirements have been strengthened are the inclusion of a user choice provision, and stricter rules for the secondary use of TDIF data (including a complete prohibition on the secondary use of biometric data).

The TDIF Privacy Requirements also require the Identity Exchange to be transparent about the secondary use of TDIF data for law enforcement purposes (e.g. the investigation of identity fraud).

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

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

12.2. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs.

There is no APP 7 'equivalent' in the TDIF Privacy Requirements. Instead, direct marketing is completely prohibited in Section 2.6 of the Privacy Requirements.

12.3. APP 7. Finding

The initial PIA (2016) recommended (R14) that the use of TDIF data for direct marketing should be prohibited.

The use of personal data for direct marketing is now completely prohibited in the TDIF Privacy Requirements (section 2.6). This is a significant privacy safeguard.

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

13.2. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs.

The APP 8 ‘equivalent’ in the TDIF Privacy Requirements is *Section 2.9 Cross border and contractor disclosure.*

It is important to note that the TDIF Privacy Requirements in section 2.9 apply to both overseas recipients and **contracted service provides, even if the data stays in Australia**.

These requirements are therefore significantly broader than APP 8 and they capture the use of all contractors (even cloud service providers retaining the data within Australia) by TDIF participants.

There is some limited scope for the cross border transfer of data in the TDIF. 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 APP 8 in the Privacy Act. The main restriction on the use of contractors is Section 2.9 of the TDIF Privacy Requirements. The following table summarises both sets of restrictions:

APP8. Cross-border Disclosure	Action / Status	Galexia Commentary
A. Has the entity identified all relevant cross border disclosure of personal information?	**In Progress**	IdPs, Relying Parties and the Identity Exchange will all need to meet this requirement. This will be assessed in the PIAs for individual participants.
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)	**Compliant**	The Initial PIA (2016) recommended (R16) that the TDIF should insist on a single approach to protecting privacy in the case of cross border data transfers. It did not recommend a complete prohibition on cross-border data transfers. The TDIF Privacy Requirements now contain a stand-alone cross border data transfer requirement, that includes a prohibition on the use of the data (by the recipient) for any purpose other than identity verification, and some specific requirements relating to enforceable contracts and audits (section 2.9). These requirements are significantly stronger than APP 8 and will ensure a more consistent application of privacy measures for cross-border transfers.
Additional TDIF Privacy Requirements (2.9) TDIF Applicants MUST ensure they have an enforceable contractual arrangement with the **contracted service provider** that specifies certain specific requirements.	**Compliant**	The TDIF Privacy Requirements in section 2.9 apply to both overseas recipients and **contracted service provides, even if the data stays in Australia.** TDIF applicants will be required to enter enforceable contractual arrangements with all contractors.
Additional TDIF Privacy Requirements (2.9) If a TDIF Applicant contracts the operation of a part of its business that relates to the TDIF it MUST make compliance with these core privacy requirements a term of the contract and ensure that the third party can be audited by the TDIF Oversight Authority (or equivalent).	**Compliant**	The TDIF Privacy Requirements in section 2.9 apply to both overseas recipients and **contracted service provides, even if the data stays in Australia.** Two key TDIF Privacy Requirements are: 1. Contractors must be bound to comply with the TDIF Privacy Requirements; and 2. Contractors must agree to be audited (if required) by the TDIF Oversight Authority (or equivalent body). These provisions represent a considerable strengthening of APP 8 and are a privacy positive feature of the TDIF.

13.3. APP 8. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.9 Cross border and contractor disclosure.*

The TDIF Privacy Requirements contain a stand-alone cross border data transfer requirement that extends the requirements to all 'contractors' even if the data is retained in Australia.

The TDIF includes a prohibition on the use of the data by recipients such as cloud service providers for any purpose other than identity verification, and also includes some specific requirements relating to enforceable contracts and audits (section 2.9).

These requirements are considerably broader and stronger than APP 8, and provide a suitable level of privacy protection.

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

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: <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 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.

APP 9 does not provide a sufficient level of privacy protection in relation to the potential use of identifiers in the TDIF, especially as Commonwealth Agencies are exempt from APP 9 (and this is likely to include the Identity Exchange and at least one Commonwealth IdP).

This was considered in the Initial PIA (2016) and specifically in recommendations R17 and R18

The TDIF Privacy Requirements now include a provision on identifiers that can be applied to all participants:

> *'An Applicant MUST NOT create a new government identifier that is used across the identity federation (ie an identifier that is sent to more than one Relying Party or Identity Service Provider)'* (section 2.10)

14.3. APP 9. Finding

The new prohibition on the use of an identifier across the identity federation represents a significant strengthening of the privacy protection measures in the TDIF. This is an essential safeguard against the use of the TDIF for general surveillance. It will also help guard against function creep (refer to 18.6.A. Guarding against function creep below) for further discussion of this issue.

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

15.3. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs. The APP 10 'equivalent' in the TDIF Privacy Requirements is *Section 2.12 Quality of personal information.*

The TDIF Privacy Requirements (section 2.12) also include specific training and audit requirements in relation to data quality at IdPs (section 2.12.1).

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 an individual's binding to photo identity documents 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.

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?	**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?	**Action Required**	The current TDIF design includes a range of measures to ensure data quality. Ensuring data quality is also included in the TDIF Privacy Requirements (section 2.12) and include specific training and audit requirements in relation to data quality at IdPs (section 2.12.1). However, an important part of APP 10 is that information should be 'up to date having regard to the purpose of the use or disclosure'. At the time of preparing this PIA, the time periods for validity and renewal of identities have not been confirmed. It will be difficult to ensure compliance with APP 10 until this issue is addressed. **Recommendation 28: Establish a time period for the validity and renewal of identity credentials** The TDIF should include a specific requirement and process for the renewal of identity credentials to ensure that information is 'up to date having regard to the purpose of the use or disclosure' of the identity information.

15.4. APP 10. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.12 Quality of personal information.* These requirements are closely aligned with APP 10 and provide a suitable level of privacy protection.

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

However, further work should be undertaken on the time periods for validity and renewal of identities and credentials – noting that it is important that identity data is up to date having regard to the purpose of the use or disclosure. (refer to Recommendation 28).

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: <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 <www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

16.3. TDIF Overview

APP 11 provides a very high level requirement that security measures are proportionate to the risk of a security breach.

APP 11 is supplemented by more detailed security requirements in the TDIF accreditation process. There are three key sets of security requirements:[19]

1. TDIF Protective Security Requirements, February 2018, version 1.0;
2. TDIF Protective Security Reviews, February 2018, version 1.02; and
3. TDIF Fraud Control Requirements, March 2018, version 1.1.

The TDIF accreditation model is a good mechanism for ensuring consistent and appropriate security measures are in place across the entire TDIF. The requirements in the three documents set out above are much more specific than APP 11.

As all TDIF applicants will be separately accredited against these higher security standards, it is not the task for this PIA to conduct a full security review of the TDIF.

Instead, this PIA briefly summarises the overall TDIF security requirements against the APP 11 requirements in the following table:

[19] Refer to Appendix – TDIF Policies and Standards.

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?	**In Progress**	The data being exchanged in the TDIF includes sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches. The TDIF accreditation requirements will help to ensure that an adequate level of security is applied to data held and transferred in the TDIF. Each accredited party will be required to undertake an initial independent security assessment, followed by regular audits. At the time of preparing this PIA, the first applicants for TDIF accreditation are starting the important process of commissioning these independent security assessments.
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	**In Progress**	IdPs and the Identity Exchange will need to meet this requirement. This will be independently assessed as part of the TDIF accreditation process for individual participants.
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	**In Progress**	IdPs and the Identity Exchange will need to meet this requirement. This will be independently assessed as part of the TDIF accreditation process for individual participants.
D. Will detailed access trails be retained and scrutinised for security breaches?	**In Progress**	IdPs and the Identity Exchange will need to meet this requirement. This will be independently assessed as part of the TDIF accreditation process for individual participants.
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	**In Progress**	IdPs and the Identity Exchange will need to meet this requirement. This will be independently assessed as part of the TDIF accreditation process for individual participants.
F. Is personal information de-identified as soon as possible?	**In Progress**	IdPs and the Identity Exchange will need to meet this requirement. This will be independently assessed as part of the TDIF accreditation process for individual participants.
G. Is a data breach response plan in place?	**In Progress**	The new *Section 2.4 Data Breach Response Management* in the TDIF Privacy Requirements sets out the steps that participants need to take to establish an appropriate data breach response plan. IdPs and the Identity Exchange will need to meet this requirement. This will be assessed as part of the PIA process for individual participants.

16.4. APP 11. Finding

APP 11 provides a very high level requirement that security measures are proportionate to the risk of a security breach. APP 11 is supplemented by more detailed security requirements in the TDIF accreditation process. The TDIF accreditation model is a good mechanism for ensuring consistent and appropriate security measures are in place across the entire TDIF. The requirements in the three documents set out above are much more specific than APP 11.

As all TDIF applicants will be separately accredited against these higher security standards, specific security measures are not considered in detail in this 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 https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

17.2. TDIF – Overview

In the TDIF Participants will be bound by the TDIF Privacy Requirements. These are slightly stronger than the APPs. The APP 12 'equivalent' in the TDIF Privacy Requirements is *Section 2.11 Access, correction and dashboard.*

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 are now required to meet the higher access standards in the TDIF Privacy Requirements (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?	**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. The Initial PIA (2016) recommended (R19) that the Identity Exchange should be required to provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transactions or identity fraud. The TDIF Privacy Requirements now include this provision: *'The Identity Exchange MUST provide individuals with access to the metadata on transactions it logs (ie that has not been deleted under its destruction policy) in a dashboard format.'* *Note: An Identity Exchange will not be able to directly identify an individual and therefore the individual will need to access its metadata by logging on through an Identity Service Provider'* (section 2.11.3).

APP 12. Access	Action / Status	Galexia Commentary
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)	**Compliant**	The TDIF Privacy Requirements include this requirement.
C. Will information be provided within 30 days?	**Compliant**	The TDIF Privacy Requirements include this requirement for all participants.
D. Will accessing personal information be provided at no cost?	**Compliant**	The TDIF Privacy Requirements include this requirement for all participants.

17.3. APP 12. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.11 Access, correction and dashboard*. These requirements are stronger than APP 12 and provide a suitable level of privacy protection.

Two key areas where the access requirements have been strengthened are the requirement for the Identity Exchange to provide a 'dashboard' for consumers, showing their recent interactions, and the introduction of more consistent measures relating to the provision of free and timely access.

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

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: <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.

All TDIF Participants will be required to meet the 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?	**Compliant**	The TDIF Privacy Requirements include a process for correcting inaccurate data. Complaints and correction requests may cause some difficulties in the TDIF, as multiple participants may each hold part of the relevant data. The Initial PIA (2016) made several recommendations (R22 and R23) to improve complaints handling processes. The TDIF Privacy Requirements now include a detailed complaints process. One important requirement is that each Participant's complaints process must be: *'integrated with other complaint handling bodies, (e.g other participants of the identity federation) so it can assist the user and refer complaints'* (section 2.13).
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)	**Compliant**	
C. UPON REQUEST ONLY Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	**Compliant**	
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?	**Compliant**	
E. Will requests for corrections be addressed within 30 days?	**Action required**	The TDIF Privacy Requirements do not include a response within 30 days for corrections to be addressed (section 2.11.2). They do include the 30 day test for Access requests (APP 12 and TDIF Privacy Requirements section 2.11.1). 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. In order to provide a consistent and high quality service to users, the TDIF Privacy Requirements should include the 30 day test for all TDIF participants. This was also a recommendation (R22) of the Initial TDIF PIA (December 2016), but has not been actioned. **Recommendation 29: Ensure a consistent timeframe for responding to complaints and correcting data** In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints and to address request to correct data within 30 days

18.4. APP 13. Finding

TDIF Participants will be bound by the TDIF Privacy Requirements in *Section 2.11.2 Correction* and Section *2.13 Handling privacy complaints*. These requirements are stronger than APP 13 and provide a suitable level of privacy protection.

One minor outstanding issue is that all TDIF applicants should be required to respond to complaint and requests to correct data within 30 days (refer to Recommendation 29).

This issue will be subject to additional assessment as TDIF Participants complete their mandatory PIAs and privacy audits.

19. Governance

The DTA recognises the importance of governance in relation to privacy protection in the TDIF, and is currently considering a range of options and governance models for the TDIF.

It is beyond the scope of this PIA to provide comprehensive advice on governance, however, some key high level governance issues have emerged during the two PIAs.

19.1. TDIF System Governance

The Initial PIA (2016) noted that many stakeholders wished to receive more detailed information on system governance arrangements for the TDIF.

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

At the time of preparing the 2018 PIA, many of the governance arrangements are not yet finalised. However, a basic outline of system governance arrangements and options is emerging:

- A. Legislation
- B. Oversight and TDIF Accreditation
- C. Binding Contractual or Operating Rules

A. Legislation

The DTA is exploring the benefits of legislation to support the TDIF, including assisting enforcement and the potential creation of an oversight authority.

There may be some privacy benefits in pursuing legislation that helps to bind TDIF Participants to the positive measures set out in the TDIF Privacy Requirements. Users may have greater confidence in the TDIF Privacy Requirements if they were referred to in some form of legislative instrument.

B. Oversight and TDIF Accreditation

The DTA is currently developing the TDIF accreditation arrangements that underpin the delivery of, and the participation in, the TDIF.

The governance arrangements, once finalised, will be administered, regulated and enforceable through an oversight body – the oversight authority. The oversight authority will also facilitate the TDIF accreditation process that applies in respect of TDIF Participants.

Parties who wish to participate will need to meet mandatory standards set out in the TDIF. They will need to be accredited against these standards upon initial application, and on an ongoing basis.

The DTA is currently considering advice and options regarding the potential establishment of an oversight authority.

C. Binding Contractual or Operating Rules

The DTA is currently considering advice and options regarding the establishment of legally binding contracts or rules. For example, legislation could set out these contractual arrangements or rules (or provide a mechanism through which the rules are established – e.g. legislative instrument).

As the contractual arrangements or rules would likely incorporate the TDIF Privacy Requirements, this will be a key privacy protection measure.

19.2. 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 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.

In practice, this separation has been achieved by the appointment of the Department of Human Services as the Identity Exchange. The DHS will not take on any role as an Identity Provider, and a range of IdPs will emerge over time.

The independence of the Identity Exchange will be enshrined in the operating rules (discussed above).

19.3. Independent TDIF Accreditation

From a privacy perspective, it will be important to ensure confidence in the TDIF 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 and other TDIF Participants. The governance report is examining ways to implement this level of independence.

19.4. Representation

All stakeholders consulted during the multi-phase PIA process and the privacy round table meetings were of the view that representation will be important to build trust and confidence in the TDIF, and to guard against changes to the privacy protections offered by the TDIF.

Stakeholders suggested that the governance arrangements should incorporate consumer engagement. This could take the form of a policy advisory committee (to advise the oversight authority). Similar models operate in other sectors (such as the ACCC Consumer Consultative Committee[20] and the ASIC Consumer Advisory Panel[21]).

Recommendation 30: Consumer and community representation in oversight of the TDIF
Consumers and community representatives should be provided with an appropriate mechanism to participate in the oversight of the TDIF. This could take the form of an advisory committee.

[20] <www.accc.gov.au/about-us/consultative-committees/consumer-consultative-committee>

[21] <asic.gov.au/about-asic/what-we-do/how-we-operate/external-committees-and-panels/consumer-advisory-panel>

19.5. Additional Measures Contained in the TDIF Privacy Requirements

The Privacy Requirements (TDIF 2018 version 1.0) include several important measures that are not strictly APP requirements. These include:[22]

- A. Privacy Champions
- B. Privacy Impact Assessments
- C. Privacy Audits

A. Privacy Champions

Each TDIF Participant must appoint a Privacy Champion (section 2.2.1). This requirement aligns with the *Australian Government Agencies Privacy Code (APS Privacy Code),*[23] but is now extended to cover all Participants (including State, Territory and private sector participants).

The designated Privacy Champion will be responsible for:

1. Promoting a culture of privacy within the Applicant that values and protects personal information.
2. Providing leadership within the Applicant's organisation on broader strategic privacy issues.
3. Reviewing and approving the Applicant's privacy management plan, and documented reviews of the Applicant's progress against the privacy management plan.
4. Providing regular reports to the Applicant's executive, including about any privacy issues arising from the Applicant's handling of personal information.

This Requirement is likely to have a positive privacy impact, especially in organisations that would otherwise not be subject to the APS Privacy Code.

B. Privacy Impact Assessments

Each System Participant must conduct a Privacy Impact Assessment (PIA) (section 2.3).

Applicants must commission a PIA to review the privacy impacts of the Applicant's TDIF related service when they first apply for TDIF accreditation. The PIA must be conducted by an independent assessor.

Participants must also conduct a PIA for all high privacy risk projects related to their TDIF services.

This Requirement is likely to have a positive privacy impact, especially in organisations who would otherwise not be subject to the APS Privacy Code (which contains similar requirements for high risk projects, but only applies to Commonwealth Agencies).

C. Privacy Audits

Each TDIF Participant must commission a Privacy Audit (Part Two of the TDIF Privacy Requirements) as part of accreditation. There are detailed requirements for who can conduct the audit, how the audit should be conducted, and how the audit should be reported.

The Privacy Audit has to be conducted following the completion of the PIA and the development of a Privacy Management Plan.

This Requirement is likely to have a positive privacy impact.

[22] This is not an exhaustive list – we have highlighted the measures that are likely to have the greatest impact.

[23] The *Australian Government Agencies Privacy Code* was registered on 27 October 2017 and commences on 1 July 2018. <https://www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/>.

19.6. Ongoing Privacy Protections

No matter how strong the initial privacy protections are at the time of the establishment of the TDIF, there will be concerns that these protections may erode over time. Stakeholders have expressed several concerns about potential future changes to the TDIF.

- A. Guarding against function creep
- B. Guarding against the development of a single identifier
- C. Guarding against the use of TDIF data for surveillance, profiling or monitoring

A. Guarding against function creep

Function creep occurs where a technology or process that is introduced for one purpose is gradually expanded or re-purposed over time. This could be through a series of small incremental/iterative changes that appear justified in isolation, but when taken together may fundamentally change the nature of the TDIF. Guarding against function creep is extremely difficult, but can usually be managed by:

1. Incorporating some of the relevant privacy protections into the fundamental design of the TDIF, so that they are difficult to remove;
    - An example of this is the implementation of the Identity Exchange as an intermediary and the role it plays in blinding other parties to the use of identities.
2. Incorporating key privacy protections into legislation or a legislative instrument, so that they cannot be removed or weakened without scrutiny;
    - This approach is the subject of Recommendation 24 in this PIA.
3. Including consumer / user representation in the oversight arrangements for the TDIF.
    - This approach is the subject of Recommendation 30 in this PIA.
4. Mandating a regular review of privacy protections in the TDIF (e.g. every three years) so that any gradual changes or proposed changes will be subject to scrutiny against the original objectives and privacy promises; and
    - This approach is the subject of Recommendation 31 in this PIA.

These options are all under consideration – none are a perfect solution to function creep, but a combination of these measures may help to prevent / deter function creep and boost confidence in the TDIF.

Recommendation 31: Mandatory review of TDIF after three years
The entire TDIF design, implementation and experience should be the subject of a major review after three years, to assess the effectiveness of privacy protections and to guard against any divergence from the original TDIF objectives and privacy promises.

There are numerous examples of similar review mechanisms enshrined in legislation, including for example the *Do Not Call Register Act* 2006 (3 years), the *Personal Property Securities Act* 2009 (3 years) and the proposed *Identity Services Matching Bill* 2018 (5 years).

B. Guarding against the development of a single identifier

Stakeholders all recognise the importance of ensuring that the System does not accidentally lead to the introduction of a single identifier in Australia. This risk is partly addressed by current measures, including:

1. A restriction in the Privacy Requirement on the use of identifiers;
2. The inclusion of the Identity Exchange as an intermediary; and
3. The choice of a federated identity model where a range of IdPs will be accredited.

However, these measures could be strengthened by additional protections. These might include:

1. Enshrining the Privacy Requirement restriction on the use of identifiers in legislation or a legislative instrument; and / or
    - This approach is the subject of Recommendation 24 in this PIA.
2. A requirement for a minimum number of IdPs to be in operation.

In this PIA we have considered the proposal to mandate a minimum number of IdPs to be in operation, but this PIA does not recommend that course of action. Our view is that strengthening other privacy protections and governance arrangements will deliver sufficient protection, and that a variety of IdPs will emerge over time. The TDIF can be tested and evaluated with only 1-2 IdPs in place. The bulk of the privacy protections offered by the TDIF come from the introduction of the Identity Exchange as an intermediary, and the strengthened Privacy Rules that apply to all accredited parties. These protections will be in place even if the number of IdPs is initially small.

C. Guarding against the use of TDIF data for surveillance, profiling or monitoring

Stakeholders all recognise the importance of ensuring that TDIF data is not used for surveillance, profiling or monitoring. This risk is partly addressed by current measures, including:

1. A restriction in the Privacy Requirement on the use of TDIF data;
2. A complete prohibition on direct marketing;
3. The TDIF Privacy Requirements include a requirement for the Identity Exchange to publish an annual Transparency Report; and
4. The inclusion of the Identity Exchange as an intermediary (especially its role in 'blinding' participants as to the identity of the IdP and Relying Party involved in transactions).

However, the TDIF does need some meta-data to be retained by the Identity Exchange in order to identify and counter identity-fraud and to investigate suspicious transactions. An entity with appropriate legal authority (e.g. a law enforcement agency with a warrant) could access the meta-data and then use that data to access additional data at IdPs and Relying Parties in order to investigate identity fraud.

This arrangement has to be maintained, but it is intended that this type of access will be rare, and will not lead to widespread surveillance or monitoring.

In order to ensure that access is limited, the following additional measure is proposed:

1. The amount of meta-data retained by the Identity Exchange will be limited (although the exact length of data retention has not yet been confirmed).
    - This approach is the subject of Recommendation 25 in this PIA.

Appendix – Acronyms

Acronym	Term	Reference
ACCC	Australian Competition & Consumer Commission	www.accc.gov.au
APP	Australian Privacy Principle	www.oaic.gov.au/agencies-and-organisations/app-guidelines/
APS	Australian Public Service	
ATO	Australian Taxation Office	www.ato.gov.au
ASIC	Australian Securities and Investments Commission	www.asic.gov.au
COAG	Council of Australian Governments	www.coag.gov.au
DHS	Department of Human Services	www.dhs.gov.au
DTA	Digital Transformation Agency	www.dta.gov.au
DVS	Document Verification Service	www.dvs.gov.au
EOI	Evidence of Identity	
FVS	Face Verification Service	www.homeaffairs.gov.au/about/crime/identity-security/face-matching-services
GUID	Globally Unique Identifier	
IdP	Identity Provider	
NIPG	National Identity Proofing Guidelines	
NISCG	National Identity Security Coordination Group	
OAIC	Office of the Australian Information Commissioner	www.oaic.gov.au
PIA	Privacy Impact Assessment	
PKI	Public Key Infrastructure	
RP	Relying Party	
TDIF	Trusted Digital Identity Framework	/www.dta.gov.au/what-we-do/platforms/identity/

Appendix – Trusted Digital Identity Framework (TDIF) Policies and Standards

As at September 2018, the framework consists of 16 documents including an overview and glossary.

These documents set the rules and standards for:

- how personal information is handled by participating government agencies and organisations
- the usability and accessibility of identity services
- how the identity system is secured and protected against fraud
- how identity services are managed and maintained
- how this framework will be managed

The TDIF Policies and Standards are available from <https://www.dta.gov.au/what-we-do/policies-and-programs/identity/join-the-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework/>.

TDIF Document	Latest Version	Drop 1 (1 Feb 18)	Drop 2 (Sept 18)
Overview and Glossary *This document provides a high-level overview of the TDIF. It outlines the relationship between the documents included in the framework, and the definition of key terms.*	v1.2	Initial Release	Update
Accreditation Process *This document defines the requirements to be met by government agencies and organisations in order to achieve TDIF accreditation for their identity service.*	v1.0	Initial Release	
Attribute Profile *This document outlines which attributes are shared between identity providers and digital services. It also includes the rules for how attributes are shared and what technical specifications they must meet.*	v1.0		Initial Release
Authentication Credential Requirements *This document sets out the authentication and credential requirements that government agencies and organisations need to meet to be accredited as Credential Service Providers under the TDIF.*	v1.3	Initial Release	Update
System Governance Interim Memorandum of Understanding *An agreement between the Digital Transformation Agency, Australian Taxation Office and Department of Human Services that sets out the interim governance and administration arrangements in relation to the TDIF.*	v2.0 (27 July 218)		Initial Release
Fraud Control Requirements *This document sets out the TDIF fraud control requirements that government agencies and organisations need to meet in order to be accredited under the TDIF.*	v1.2	Initial Release	Update
Identity Proofing Requirements *This document sets out the identity proofing requirements that government agencies and organisations need to meet to be accredited as Identity Service Providers under the TDIF.*	v1.07	Initial Release	Update
OpenID Connect 1.0 Profile *This document provides the OpenID Connect 1.0 Profiles for interactions between:* • *a relying party and an identity exchange* • *an identity provider and an identity exchange*	v1.0		Initial Release

TDIF Document	Latest Version	Drop 1 (1 Feb 18)	Drop 2 (Sept 18)
Privacy Requirements *This document sets out the TDIF privacy requirements that government agencies and organisations need to meet in order to be accredited under the TDIF. These requirements incorporate the Privacy Act 1988 and the Australian Privacy Principles, state-based privacy legislation and privacy best practice.* **Contents** ● 1 Introduction ● 2 Part one: Privacy requirements ○ 2.1 General requirements ○ 2.2 Privacy governance ■ 2.2.1 Roles ■ 2.2.2 Policies ■ 2.2.3 Internal privacy capability ○ 2.3 Privacy Impact Assessment ○ 2.4 Data Breach Response Management ○ 2.5 Notice of Collection ○ 2.6 Collection and use limitation ■ 2.6.1 Identity Exchange additional requirements ○ 2.7 Collection and use of biometrics ○ 2.8 Consent ■ 2.8.1 Identity Service Provider additional requirements ○ 2.9 Cross border and contractor disclosure ○ 2.10 Government Identifiers ○ 2.11 Access, correction and dashboard ○ 2.11.1 Access ○ 2.11.2 Correction ○ 2.11.3 Dashboard ○ 2.12 Quality of personal information ○ 2.11 Identity Service Provider additional requirements ○ 2.13 Handling Privacy Complaints ○ 2.14 Destruction and de-identification ● 3 Part two: privacy audit ○ 3.1 Purpose and context of the privacy audit ○ 3.2 Privacy audit process ○ 3.3 Type of audit and auditor's skills ○ 3.4 Privacy audit roles and responsibilities ■ 3.4.1 Trust Framework Accreditation Authority ■ 3.4.2 The Applicant ■ 3.4.3 Authorised Assessor ● References ● Annex A: Privacy audit template	v1.0	Initial Release	
Protective Security Requirements *This document sets out the TDIF protective security requirements that government agencies and organisations need to implement in order to be accredited under the TDIF.*	v1.0	Initial Release	
Protective Security Reviews *This document outlines the protective security reviews that will be performed on an identity service as part of the TDIF accreditation process.*	v1.03	Initial Release	Update
Risk Management Requirements *This document sets out the TDIF risk management requirements that government agencies and organisations need to meet in order to be accredited under the TDIF. This document also explains an approach to risk management that agencies and organisations can use to meet the requirements.*	v1.0	Initial Release	

TDIF Document	Latest Version	Drop 1 (1 Feb 18)	Drop 2 (Sept 18)
SAML 2.0 Profile *This document provides the SAML 2.0 Profile for interactions between:* ● *a relying party and an identity exchange* ● *an identity provider and an identity exchange*	v1.0		Initial Release
Service Operations Testing Requirements *This document sets out the TDIF operational testing requirements that government agencies and organisations need to meet in order to be accredited under the TDIF. These requirements include service design, service transition and service operations.*	v1.0		Initial Release
Technical Integration Testing Program *This document sets out the TDIF integration testing requirements that government agencies and organisations need to meet in order to be accredited under the TDIF. These requirements include the processes needed to run an effective technical integration testing program.*	v1.0		Initial Release
Usability and Accessibility *This document defines the usability and accessibility requirements that government agencies and organisations need to meet in order to be accredited under the TDIF. These requirements ensure that identity services are simple and easy to use.*	v1.0	Initial Release	

Appendix – DTA Response to the Second Independent TDIF Privacy Impact Assessment

Refer also to 1.6. DTA Privacy Work Plan for progress against recommendations from the December 2016 PIA[24].

Component / APP	Galexia Recommendation	DTA Response
Component 1 – Mandatory policies and standards	**Recommendation 24:** The TDIF Privacy Requirements should be strengthened by enshrining them in a legislative instrument	**Agree** – the Requirements should be strengthened
DTA Comment: We agree that the Privacy Requirements in the TDIF should not change without community consultation and only after ensuring the changes are privacy protective. The DTA is reviewing the benefits of legislation to support the TDIF, including to enshrine privacy protections. The DTA will explore ways to enshrine the TDIF Privacy Requirements in a 'strong instrument' including a legislative instrument or binding contractual rules.		
Component 2 – The Identity Exchange	**Recommendation 25:** The Identity Exchange should only retain metadata for a short period	**Need to explore further**
DTA Comment: We agree that we need to set a maximum period for retention of transaction data related to individual's transactions in the Exchange. The Oversight Authority will need to access or obtain data of transactions for evidence (ie evidence someone consented to a transaction) in investigations of complaints and fraud. Our current use cases suggest transaction data would need to be retained for longer than 18 months. There will be some data that needs to be retained indefinitely for the person to use the system such as the links to their relying party services and IDPs and consent preferences. The DTA needs to do more work to test the use cases against the retention period and also understand what pieces of data need to be retained under the Archives Act and under the Information Security Manual.		
APP 1 – Open and transparent management	**Recommendation 26:** The Identity Exchange and accredited IdPs should develop stand-alone privacy policies	**Agree**
DTA Comment: We will make this a requirement in the next iteration of the privacy requirements		
APP 3 – Collection of solicited personal information	**Recommendation 27:** Strengthen the TDIF governance arrangements to ensure that the requirements on biometrics receive suitable legislative backing	**Agree**
DTA Comment: We agree that the Privacy Requirements in the TDIF should not change without community consultation and only after ensuring the changes are privacy protective. The DTA is reviewing the benefits of legislation to support the TDIF, including to enshrine privacy protections. The DTA will explore ways to enshrine the Privacy Requirements – particularly those around biometrics - in a strong instrument, including a legislative instrument or binding contractual rules.		
APP 10 – Quality of Personal Information	**Recommendation 28:** Establish a time period for the validity and renewal of identity credentials	**Agree**
DTA Comment: We will include a time period for the validity and renewal of identity credentials in near term iteration of the proofing requirements.		
APP 13 – Correction	**Recommendation 29:** Ensure a consistent timeframe for responding to complaints and correcting data	**Agree**
DTA Comment: Agree.		

[24] Recommendation numbering is continued from the initial TDIF PIA (December 2016) <https://www.dta.gov.au/files/DTA_TDIF_Alpha_Initial_PIA.pdf.

Component / APP	Galexia Recommendation	DTA Response
Governance	**Recommendation 30**: Consumer and community representation in oversight of the TDIF	**Agree**
DTA Comment: The DTA has consulted across privacy and community groups in the development of the TDIF. We will ensure consumer and community groups are represented in the oversight of the TDIF.		
Governance	**Recommendation 31**: Mandatory review of TDIF after three years	**Agree**
DTA Comment: We agree to a review three years after our first public beta service.		