galexia

dta

Commonwealth Digital Transformation Agency (DTA)

3rd Independent Privacy Impact Assessment (PIA)

on the

TDIF and related Digital Identity Eco-system (as of September 2020)

Report Date: March 2021

DTA Response: October 2021

[v13b 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: manage@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 on developments around the Trusted Digital Identity Framework (TDIF) and the related digital identity ecosystem. This PIA covers the period from September 2018 (PIA2) to September 2020. Specific consideration of the proposed Digital Identity Legislation and the November 2020 Consultation Paper (and subsequent ones) <www.digitalidentity.gov.au/have-your-say> is not within the scope of this PIA.

Document Identification

Document title	DTA – 3rd Public PIA on the Digital Identity Eco-system (September 2018 to September 2020)
Document filename	gc609_dta_tdif_2020_pia3_v13b_dta_rec_response_20211025_FINAL.pdf

Client Details

Digital Transformation Agency (DTA)
Australian Government
<www.dta.gov.au> and <www.digitalidentity.gov.au>

Advisor Details

Galexia Contact

Galexia <www.galexia.com>
Level 11, 175 Pitt St, Sydney NSW 2000, Australia
p: +612 9660 1111
e: manage@galexia.com

Peter van Dijk (Managing Director)
m: +61 419 351 374

Galexia Reference	GC609
Project emails	dta@galexia.com (Galexia and DTA)

Contents

1. Overview

1.1. Approach

Galexia <www.galexia.com> has completed this Third Privacy Impact Assessment (PIA) for the Digital Transformation Agency (DTA) <www.dta.gov.au>.

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by further developments around the Trusted Digital Identity Framework (TDIF) and the related digital identity ecosystem since the Second PIA (September 2018) and until September 2020. The focus is on changes to the TDIF documentation and implementation aspects of the TDIF that have been proposed or developed since the second PIA.

This PIA is the **third** step in a multi-phase and independent PIA process commissioned by the Digital Transformation Agency.

We consider that it is important to consider the sequence of privacy assessments – including assessment of key TDIF Privacy Requirements against each of the APPs (as undertaken in the first two PIAs) – and therefore believe it is critical to consider the package of recommendations that have been developed across all of the PIAs. While this PIA is careful not to make the same findings and recommendations of earlier public PIAs, we do refer to specific recommendations that remain relevant.

DTA has developed a separate privacy work plan (and traceability matrix) to monitor progress against all of the privacy recommendations and to consider earlier findings and observations against new proposals – and where necessary commission additional PIAs.

A. Initial PIA (December 2016)

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);[1]

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 the second PIA: **3**

Refer to Initial PIA Recommendation Summary in Appendix 4.

B. Second PIA (September 2018)

A second independent public PIA on the planned implementation of the Trusted Digital Identity Framework (TDIF) as of September 2018;[2]

The second public PIA built on work undertaken in the initial PIA and used the consistent section headings and follow-on recommendation numbering system, ensuring integrity and traceability across a series of public PIAs.

In total, the second PIA (December 2018) made 8 recommendations. They have been addressed as follows:

- Accepted and commitment to implement: **7**
- Deferred for further consideration: **1**

Refer to Second PIA Recommendation Summary in Appendix 4.

[1] Available from <www.digitalidentity.gov.au/privacy-and-security/privacy>.

[2] Ibid.

C. Third PIA (as of September 2020) – This PIA

A third independent public PIA on developments to the Digital Identity Eco-system as of September 2020 (this PIA).

This PIA has particular focus on new or changed features of the Trusted Digital Identity Framework (TDIF) and the Digital identity ecosystem – specifically, proposed implementation approaches since the second PIA and encompassing both changes from TDIF3 to TDIF4 and governance and operational proposals.

This PIA considers the Digital Identity program as a whole and, given the earlier PIAs, focuses on changes (or proposed changes) to the TDIF/product design (including extra attributes, deduplication, biometric collection restrictions, more mature governance concepts and practice).

In total, this third PIA has made 35 recommendations – and all have been accepted and with commitment to implement. A small number have been noted for future consideration where functionality is a possible future area of functionality.

Refer to Section 2. PIA3 Recommendation Summary and DTA response (October 2021).

As part of this PIA Galexia engaged with selected stakeholders, through a targeted survey and individual follow-up. This process was not without its challenges. The survey approach was a useful mechanism for Galexia to work with DTA to articulate 9 key implementation issues and proposed approaches to resolving these issues. The feedback provided by stakeholders in the survey has been shared with DTA and, where appropriate, reflected in the relevant sections of this PIA. Refer to Appendix 6 – Stakeholders.

Many issues were the subject of findings and recommendations in the first and second PIAs and while this PIA does not create a duplicate recommendation it does refer to the recommendations from the earlier PIAs.

This PIA considers compliance with privacy legislation and relevant privacy measures contained in the TDIF documentation and interim Governance arrangement.

Information contained in this PIA is based on:

- Meetings with the DTA, including senior management, technical staff, and policy staff;
- Stakeholder consultation and responses to Stakeholder Survey;
- Meetings with TDIF Participants and external stakeholders (2018-2020);
- Documentation and agreements;
- General research and literature review on privacy and identity verification issues; and
- Review of relevant privacy legislation and guidelines.

1.2. Agreed Scope for PIA3

In Scope	Out of Scope
● High-level identification of potential compliance issues in the context of the Commonwealth privacy legal framework	● Compliance with specific sectoral legislation or State and territory legislation (although some key issues may be identified and flagged for further review)
● Review of *key* documents, with a focus on changes to TDIF since the previous PIAs were conducted	● Review of the entire suite of DTA documentation
● Internal stakeholder consultation ● Targeted external consultation based on a Survey and direct engagement with stakeholders	● Extensive public consultation
● Brief consideration of security issues relevant to privacy compliance	● Detailed security assessment
● Review any relevant research into likely community opinion	● Detailed study or assessment of public attitudes
● Consider the Digital Identity program as a whole, but given 2 previous PIAs, focus on changes to the TDIF/product design (extra attributes, deduplication, biometric collection restrictions, more developed governance concepts and practice)	● Detailed consideration of the content of proposed primary legislation or legislative drafting, ● Consideration of audits of currently accredited participants
● Tracking progress on recommendations from the earlier PIAs	● Revisiting ground covered by the earlier PIAs

2. PIA3 Recommendation Summary and DTA response (October 2021)

Please note that this PIA continues the numbering of recommendations from PIA1 and PIA2 – and hence the first recommendation in this PIA starts at Recommendation 32. Refer to Appendix 4 – Initial and Second PIA Recommendation Summary for Recommendations 1-31.

The DTA has provided a formal response to the recommendations in this PIA – the recommendations and DTA's responses are extracted below:

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
Ongoing consideration of privacy and updates to the TDIF	**Recommendation 32:** Continue to consider recommendations from prior PIAs when making changes to the TDIF and implementing aspects of the digital identity ecosystem that may impact upon privacy The findings and recommendations from all of the PIAs can be seen as a package. Privacy risks identified in each of the PIAs should be monitored to ensure that they are being addressed on a continuous basis. Subsequent review of privacy issues and PIAs should not need to make these recommendations again. Continue to maintain traceability and consider public commitments to recommendation responses and publish any changes	**Agree** DTA understands the value of PIAs, which is why it has commissioned a series of independent PIAs on this project. This is the third PIA on the digital identity project, with a fourth PIA currently underway on the proposed digital identity legislation. This said, our previous PIAs are important artefacts in our work, in particular in shaping the policy thinking behind the TDIF and the additional privacy protections in the Trusted Digital Identity Bill. All our previous PIAs on the project remain publicly accessible on the Digital Identity website,[3] indicating our commitment to transparency and traceability.
Updates to the Privacy Requirements in the TDIF	**Recommendation 33:** Document changes to the TDIF and consider and communicate possible privacy impacts To support openness and transparency it is important to continue to engage with stakeholders about proposed updates and identify and explain the impacts of both individual changes and also the sum of those changes. Consideration of privacy may extend beyond the Privacy Requirements section in the TDIF.	**Agree** The TDIF has been incorporated into the Trusted Digital Identity Bill and the draft TDIF Accreditation Rules, which were recently released for public consultation (the third round of consultation on digital identity legislation). Enshrining the TDIF into these legislative instruments will mean that formal consultation (and in the case of the Bill, parliamentary scrutiny) will need to occur before the rules can be changed. This means that changes to the rules will receive a high level of public scrutiny, and any changes will necessarily need to be documented. Between Oct-Dec 2021, the TDIF will only be changed to align to feedback received on the TDI Bill and Accreditation Rules. All changes will be made as 'emergency changes'. Before the Bill and Rules are passed into law, changes to the TDIF will be made in accordance with the TDIF Change Process, which is available publicly on the Digital Identity website: Trusted Digital Identity Framework | Digital Identity.[4] Detailed changes across all TDIF documents are recorded in the Change Log spreadsheet, also available on the website. All changes are communicated with a notification email to accreditation holders, applicants and other stakeholders upon publication.

[3] <www.digitalidentity.gov.au/privacy-and-security/privacy>

[4] <www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework>

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
Section 5. Nine Key Implementation Issues considered in this PIA		
A. Enduring Consent: A proposal to allow Users to provide enduring consent to the sharing of core data		
APP 1: Open and Transparent Management of Personal Information	**Recommendation A1:** Relevant TDIF Participants (Identity Exchange) will need to update privacy policies to describe the process for withdrawing enduring consent.	**Agree** This is specifically dealt with in the draft TDIF Accreditation Rules (part of the proposed Digital Identity legislation). Specifically, there is a proposed rule requiring accredited entities to allow individuals to withdraw their consent, and to include a clear description of this process in their privacy policy (see Chapter 4, Part 3, 3.9 (3)-(5)). It should be noted that under existing processes for the TDIF accreditation scheme, privacy policies and notices are reviewed during the accreditation process and then annually. This process of yearly review will continue if the Rules above become law to ensure ongoing and thorough review of these privacy artefacts.
APP 5: Notification	**Recommendation A2:** Update notices for relevant TDIF Participants (Identity Exchange) to support enduring consent. The key requirements for the privacy notices include: – Use of plain, clear language; – Clarification that enduring consent is optional; – Information on the consequences of granting / not granting enduring consent; and – Information on the ability (and process) for withdrawing enduring consent at any time.	**Agree** This is specifically dealt with in the draft TDIF Accreditation Rules (part of the proposed Digital Identity legislation). Specifically, draft Rule 3.9 (4) in Chapter 4, Part 3 requires an entity which obtains enduring consent from a user to, at the time of obtaining the enduring consent: (a) notify the user that such consent is optional; and (b) provide the user with a clear description of the impact of providing and of not providing such consent; and (c) inform the user of the process for the user to withdraw or vary such consent. It should be noted that under existing processes for the TDIF accreditation scheme, privacy policies and notices are reviewed during the accreditation process and then annually. This process of yearly review will continue if the Rules above become law to ensure ongoing and thorough review of these privacy artefacts.
B. User Managed Digital Identity: A proposal to facilitate User management of their Digital Identity		
APP 1: Open and Transparent Management of Personal Information	**Recommendation B1:** Develop and publish clear documentation of the proposed Individual History Log functionality There may need to be multiple versions, including: – technical documentation for implementing participants (the Exchange) – clear and easy-to-understand explanation to individuals, including articulation of benefits and protections.	**Agree** (note – individual history log is now referred to as 'user dashboard' in the Digital Identity legislation) The proposed functionality is described in the TDIF Accreditation Rules (part of the proposed Digital Identity legislation) which was recently released for public consultation. Specifically, draft Rule 6.4 in Chapter 5, Part 6 requires accredited identity exchanges to have a user dashboard which: • Displays the user's consumer history • Enables the user to view the express consents provided by the user • Does not store a user's attributes after the user has ceased using the user dashboard The Rules, if they become law, will be publicly accessible, and will not be able to be amended without public consultation. Further work will be undertaken on the implementation of the dashboard, including further documentation for participants and users.

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
APP 1: Open and Transparent Management of Personal Information	**Recommendation B2:** Review relevant public facing Accredited TDIF participant privacy policies and notices for changes required due to the introduction of the Individual History Log functionality In order to ensure that consumers are not misled by existing statements, review any relevant public facing Accredited TDIF participant privacy policies and notices to ensure that existing statements or promises on information collection, use and disclosure do not require amendment following the introduction of Individual History Log functionality.	**Agree** The Digital Identity legislation enshrines a stringent accreditation process involving review of applicants' privacy artefacts. In addition, accredited entities must undertake a yearly privacy assessment which must include an assessment of how the entity is complying with its obligations under the legislation, including in relation to privacy notices and policies. It should be noted that under existing processes for the TDIF accreditation scheme, privacy policies and notices are also reviewed during the accreditation process and then annually. Our team will specifically review relevant identity exchange privacy policies and notices to ensure that they adequately describe processes in the relation to the user dashboard.
APP 11: Security	**Recommendation B3:** The Individual History Log functionality should be the subject of a detailed security assessment and strict security measures that reflect the high likelihood of attacks against this mechanism.	**Agree** The Digital Identity legislation creates a stringent accreditation process involving strict protective security requirements which applicants must meet. Prior to the passage of legislation, this detailed security assessment will be provided by the protective security requirements in the TDIF which are considered during the current accreditation process.
APP 11: Security	**Recommendation B4:** Develop the data retention policy requirements to be applied to the Centralised User Management Interface to provide access to recent transactions or a maximum number of transactions. The exact number can be set following security assessments and user trials.	**Agree** The Digital Identity legislation creates high level rules relating to record keeping and data retention, including maximum retention periods. Further work will be undertaken on the implementation of the dashboard, including the volume of data it can store. Solutions must balance reasons for lower volume of data (including data minimisation and privacy) against reasons for higher volume of data (including ease of user access to their records and freedom of information rights).
C. Deduplication: A technical solution to facilitate identity resolution		
APP 1: Open and Transparent Management of Personal Information	**Recommendation C1:** Develop and publish clear documentation and guidance of the Identity Deduplication functionality There may need to be multiple versions, including: – technical documentation for implementing participants – clear and easy-to-understand guidance to individuals, including articulation of benefits and protections.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication plays any role in the Australian Government Digital Identity System, then we will ensure that there is sufficient privacy protection for users, including adequate documentation for participants and users.
APP 1: Open and Transparent Management of Personal Information	**Recommendation C2:** Review relevant public facing Accredited TDIF participant privacy policies and notices In order to ensure that consumers are not misled by existing statements, review any relevant public facing Accredited TDIF participant privacy policies and notices to ensure that existing statements or promises on information collection, use and disclosure do not require amendment following the introduction of deduplication.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication plays any role in the Australian Government Digital Identity System, then we will ensure that there is sufficient privacy protection for users, including review of participant privacy policies and notices. It should be noted that under existing processes for the TDIF accreditation scheme, privacy policies and notices are reviewed during the accreditation process and then annually. This process of yearly review will continue if the Digital Identity legislation becomes law to ensure ongoing and thorough review of these privacy artefacts.

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
APP 6: Use or Disclosure	**Recommendation C3:** Update the TDIF to include a specific section on the deduplication data – including a list of permitted uses of the data and a list of prohibited uses.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication plays any role in the Australian Government Digital Identity System, then we will ensure that there is sufficient privacy protection for users, including through rules tailored to deduplication (assuming more general rules cannot accomplish the same purpose). Notably, the Trusted Digital Identity Bill already contains rules on permitted and prohibited uses on particular types of data, as does the existing TDIF.
APP 10: Quality of Personal Information	**Recommendation C4:** The deduplication solution should be subject to trials and evaluations to ensure an acceptable degree of data accuracy, prior to full implementation of the solution.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication is further pursued, then it will proceed through trials.
APP 11: Security	**Recommendation C5:** Include the deduplication solution in the high-level DTA security review of the TDIF environment.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication is further pursued, then it will be included in future security reviews.
APP 11: Security	**Recommendation C6:** Add the deduplication solution to the security audit requirements for Accredited TDIF participants.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication plays any role in the Australian Government Digital Identity System, then we will ensure that there is sufficient privacy protection for users, including through rules tailored to deduplication (assuming more general rules cannot accomplish the same purpose). Notably, the Trusted Digital Identity Bill and draft TDIF Accreditation Rules already contain stringent security audit requirements for entities seeking accreditation which would cover deduplication processes, as does the existing TDIF.
Governance: CoI Document Custodians	**Recommendation C7:** The DTA TDIF team should consult with State and Territory CoI owners on the potential use of their document identifiers in the deduplication solution.	Note Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. In any case, consultation on this issue was conducted with the jurisdictions for TDIF Release 4.

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
Governance: TDIF Policies	**Recommendation C8:** The entire suite of TDIF documentation should be the subject of a brief review to assess the impact of deduplication, and updated as necessary.	**Note** Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution. If deduplication plays any role in the Australian Government Digital Identity System, then we will ensure that the relevant rules are updated as necessary.
D. Restricted Attributes: A policy solution to establish a process for Relying Parties to seek additional and restricted attributes.		
APP 3: Collection of solicited personal information	**Recommendation D1:** Develop and publish clear attribute authorisation rules that incorporate data minimisation principles RPs that require additional restricted attributes should justify their request and this could be included in attribute authorisation rules that incorporates data minimisation, including 3 tests: **1)** Justification of restricted attributes **2)** Demonstrate how the request for restricted attributes will meet a legislative or regulatory requirement **3)** Require that the restricted attributes will not be extended beyond those collected by IdPs in the normal course of verifying an identity	**Agree** Rules governing the use of restricted attributes are contained in the Trusted Digital Identity Bill. In line with the principle of data minimisation, the rules in the Bill: • require relying parties to have authorisation from the Oversight Authority before they can receive such restricted attributes (i.e. they do not have access to restricted attributes by default) • define restricted attributes to include information such as tax file numbers (TFNs), medicare numbers and all health information instead of leaving the categories of restricted attributes to be defined by the Minister (i.e. meaning more information is subject to the greater level of protection, and that this occurs from the moment the Bill takes effect).
APP 11: Security	**Recommendation D2:** Review security measures for sharing restricted attributes Consider the proposed use of restricted attributes in the high-level security review of the digital identity environment.	**Agree** The security measures for sharing of restricted attributes were considered through: • security reviews conducted during the course of the building of the Australian Government Digital Identity System • the consultation processes for both the existing TDIF and the Digital Identity Legislation
Governance: Public register	**Recommendation D3:** Public register of shared restricted attributes The OA should develop and maintain a public register of all restricted attributes that have been authorised to be shared with specific RPs. The OA should consider extending this register to include proposed authorisations.	Agree The Trusted Digital Identity Bill establishes two public registers to ensure transparency and public trust. Relevantly, the TDIS register will contain many details relating to participating relying parties, including the restricted attributes they are authorised to obtain (which will be listed as conditions on their onboarding).
Governance: Exceptions	**Recommendation D4:** Clarify exceptions to the authorisation requirements The TDIF should clarify the circumstances in which attributes can be shared with RPs without requiring authorisation.	**Agree** It should be noted that entities cannot onboard to the Australian Government Digital Identity System as a participating relying party without going through a stringent application process. The Trusted Digital Identity Bill makes it a civil penalty offence to onboard without the required approvals. The attributes that can be shared after an entity has been accepted for onboarding are clearly listed in the TDIF (and the proposed TDIF Accreditation Rules).

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
Governance: Managing Function Creep	**Recommendation D5:** Expand authorisation requirements to manage function creep Expand the authorisation requirements for sharing restricted attributes to include additional precautions against function creep. This should include: **1)** Clarifying that authorisations are not precedent setting **2)** Prohibiting retrospective authorisations **3)** Encouraging a review of authorisations every three years **4)** Imposing strict data retention requirements **5)** Limiting justifications to specific RP legislation and business needs **6)** Clarifying excluded attributes	**Agree** Enshrining the rules governing restricted attributes in the Trusted Digital Identity Bill provides these rules a level of protection against function creep because: • the Bill cannot be changed without Parliamentary scrutiny • the legislation gives decision-making power in relation to conditions to the Oversight Authority, ensuring that an independent decision maker assesses every request for restricted attributes on its merits (i.e. no precedent setting) • the conditions applicable to an entity can be changed at any time on its own initiative (i.e. the OA can act immediately instead of waiting for a review period) • there are no retrospective authorisations by the Oversight Authority. On top of the rules related to restricted attributes, the Bill also contains specific record keeping and data retention requirements. Finally, the Bill excludes certain types of information (such as racial or ethnic origin, political opinion or religious belief) from the definition of attribute. This ensures that such information cannot be used in a digital identity system by an accredited entity. These excluded attributes are listed in s 10(3)(c) of the Bill.
E. Biometrics: Proposal to manage the use and retention of biometric data presented during proofing		
APP 1: Open and Transparent Management of Personal Information	**Recommendation E1:** Identity Provider privacy policies should be reviewed to ensure that promises made about biometric image matching remain accurate. This is required as Identity Providers are permitted to use one-to-one matching between the presented image and an image stored in the RFID chip of an identity document.	**Agree** As above, under existing TDIF accreditation processes, review of privacy policies and notices occurs at the accreditation stage and then annually. This process of yearly review will continue if the Digital Identity legislation becomes law to ensure ongoing and thorough review of these privacy artefacts. In addition, it is intended that the Trusted Digital Identity Bill will contain a range of stringent safeguards on biometric information, including but not limited to: • prohibiting disclosure to law enforcement • prohibiting disclosure to relying parties • preventing one-to-many matching (i.e. conducting a general database search to find a match against a particular identity) • requiring express consent before collection, use or disclosure
APP 5: Notification	**Recommendation E2:** Review and update Identity Provider privacy notices to reflect the potential use of images contained in RFID chips of Identity documents.	**Agree** As above, under existing TDIF accreditation processes, review of privacy policies and notices occurs at the accreditation stage and then annually. This process of yearly review will continue if the Digital Identity legislation becomes law to ensure ongoing and thorough review of these privacy artefacts. In addition, it is intended that the Trusted Digital Identity Bill will contain a range of stringent safeguards on biometric information, including but not limited to: • prohibiting disclosure to law enforcement • prohibiting disclosure to relying parties • preventing one-to-many matching (i.e. conducting a general database search to find a match against a particular identity) • requiring express consent before collection, use or disclosure

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
APP 11: Security	**Recommendation E3:** The security arrangements for the collection, storage and destruction of biometric information should be reviewed and updated to reflect the proposed use of images contained in RFID chips of Identity documents.	**Agree** The protections relating to biometric information in the Trusted Digital Identity Bill include the following: • requiring express consent before collection, use or disclosure • for identity service providers, requiring deletion once verification is complete (subject to exception on testing below) • for credential service providers, requiring deletion if an individual withdraws consent (subject to exception on testing below) • limiting collection to accredited identity service providers and accredited credential service providers only. The Bill allows for retention of *biometric information* in narrow circumstances to enable limited operational testing and fraud detection activities. The Bill and TDI rules place controls on such testing, including requirements for: • approval from the *Oversight Authority* • testing plans • only certain kinds of testing to be undertaken • deletion of biometric information after 14 days.
F. Governance Oversight: A staged approach to the management of key privacy issues via governance and oversight mechanisms.		
Recommendations from earlier PIAs and DTA's response remains current, including: • **PIA1 – Recommendation 23:** Governance arrangements • **PIA2 – Recommendation 24:** The TDIF Privacy Requirements should be strengthened by enshrining them in a legislative instrument • **PIA2 – Recommendation 30:** Consumer and community representation in oversight of the TDIF • **PIA2 – Recommendation 31:** Mandatory review of TDIF after three years		
G. Fraud Management: A policy and technical proposal to enhance the fraud management function in Stage 1 of the Digital Identity system.		
APP 1: Open and Transparent Management of Personal Information	**Recommendation G1:** Key TDIF Participants (IdPs and the Exchange) should update privacy policies to be open about the use of some digital identity system data for fraud management. The privacy policies should disclose (or link to) the data fields that might be shared for fraud management and the data retention periods that apply to this activity.	**Agree** Current TDIF participants are already required to include a statement in their privacy notices that they may use personal information as required by the TDIF, including for the purposes of detecting, managing and investigating fraud. In addition, current participants have been specifically advised to update their existing privacy notice to inform users that their information may be shared with the Interim Oversight Authority. As above, under existing TDIF accreditation processes, review of privacy policies and notices occurs at the accreditation stage and then annually. This process of yearly review will continue if the Digital Identity legislation becomes law to ensure ongoing and thorough review of these privacy artefacts. It is intended that the Trusted Digital Identity Bill will contain specific rules on law enforcement access to information, including a prohibition on disclosure of biometric information to law enforcement.

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
APP 1: Open and Transparent Management of Personal Information	**Recommendation G2:** The Oversight Authority should publish a user guide to fraud management in the digital identity system to enhance consumer understanding and awareness. The user guide could be in the form of an FAQ with information and links on how to report a suspicious transaction or other concerns regarding fraud.	**Agree** Digitalidentity.gov.au includes a range of information that supports users when a fraud and cyber event is suspected. Further, the OA's Participant Handbook includes a full chapter of fraud and cyber security management and response processes, including reporting, remediation and victim help. This information is used by participants to help them craft their user communications (e.g. their terms and conditions of use). All these materials will be updated from time to time as necessary, including being updated if changes to processes occur as a result of the PIA into the Data Sharing Framework. replicated on the OA's future website, the recommendation is achieved. We will generally continue to ensure that adequate user materials and education exists.
APP 3: Collection of solicited personal information	**Recommendation G3:** In order to comply with the data minimisation requirements in APP 3 and the TDIF, the amount of information collected for fraud management purposes should be limited. Some further guidance is provided below (refer to Recommendations G9 and G10 below) on the types of information that should not be collected.	**Agree** The proposed Data Sharing Framework to be used by the Oversight Authority and participants in situations of suspected fraud is currently the subject of a privacy impact assessment (PIA) to ensure that privacy considerations are adequately considered. This PIA will necessarily consider compliance with the APPs, including the data minimisation requirements in APP 3. The finding of the PIA is due in late 2021. Once the findings of the PIA are delivered, we will continue to work on the Data Sharing Framework, including ensuring appropriate levels of data minimisation. It should be noted also that: • The existing Services Australia identity exchange will be required to undertake technical blinding under the Digital Identity legislation. This protection will be contained as a condition on Services Australia's accreditation from the commencement of the Act. • More broadly, the design of the Australian Government Digital Identity System has been heavily informed by data minimisation principles since its inception.
APP 5: Notification	**Recommendation G4:** Where a TDIF participant makes a specific reference to the double blind as a privacy enhancing feature, their Privacy Notice must disclose that the double blind can be lifted for fraud management purposes. This Recommendation may need to be implemented on a case-by-case basis, as not all TDIF participants refer to the double blind arrangements.	**Agree** Current TDIF participants are already required to include a statement in their privacy notices that they may use personal information as required by the TDIF, including for the purposes of detecting, managing and investigating fraud. In addition, current participants have been specifically advised to update their existing privacy notice to inform users that their information may be shared with the Interim Oversight Authority. As above, under existing TDIF accreditation processes, review of privacy policies and notices occurs at the accreditation stage and then annually. This process of yearly review will continue if the Digital Identity legislation becomes law to ensure ongoing and thorough review of these privacy artefacts. It should be noted that only the existing Services Australia identity exchange will be required to undertake technical blinding under the Digital Identity legislation. This protection will be contained as a condition on Services Australia's accreditation from the commencement of the Act. The privacy policy of the Services Australia identity exchange will be reviewed (like all participants' policies) to ensure that there is adequate disclosure of fraud management processes.

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
APP 11: Security	**Recommendation G5:** The digital identity system fraud management solution should be subject to an independent security review.	**Agree** The proposed fraud and cyber security management solution (Oversight Authority Response System or OARS) to be used by the Oversight Authority and Participants of the Digital Identity system is currently the subject of a privacy impact assessment (PIAs) to ensure that privacy considerations are adequately considered. The preliminary PIA has recommended a full security review of the OARS, which has been supported by Services Australia. Once the findings of those two PIAs are delivered, the framework will also undergo a formal security review.
APP 11: Security	**Recommendation G6:** The digital identity system fraud management solution should be subject to a formal data retention policy that requires data to be destroyed once it is no longer required for investigations, enforcement or further analysis. In some cases it may be appropriate to de-identify the data.	**Agree** The proposed fraud and cyber security management solution (Oversight Authority Response System or OARS) to be used by the Oversight Authority is currently the subject of a privacy impact assessment (PIAs) to ensure that privacy considerations are adequately considered. The PIA will necessarily consider APP issues including destruction and de-identification of data. The preliminary PIA has recommended a data retention policy be developed for OARS, which has been supported by Services Australia.
Governance: Consultation	**Recommendation G7:** Include fraud management issues in the scheduled stakeholder consultation rounds (such as consideration of the legislative package).	**Agree** Fraud management has been considered in our stakeholder consultation during each of the three rounds of consultation on the legislation.
Governance: Managing Function Creep	**Recommendation G8:** Steps should be taken to manage concerns regarding function creep in relation to fraud management. These should include: **– Measure 1:** Define and restrict the exact categories of fraud that may trigger lifting the double blind **– Measure 2:** Establish regular reviews of the fraud management system **– Measure 3:** Conduct a Privacy Impact Assessment (PIA) on the fraud analytics process	**Agree** The purpose of the proposed Data Sharing Framework (DSF) to be used by the Oversight Authority and Participants of the Digital Identity system is to prevent function creep by clearly stating when data can be shared for fraud prevention purposes. This DSF is currently the subject of PIA to ensure that privacy considerations are adequately considered. These PIAs will necessarily consider compliance with the APPs, including the data minimisation requirements in APP 3. Once the findings of those two PIAs are delivered, we will continue to work on the framework, including ensuring appropriate levels of oversight to prevent function creep.
Double blind	**Recommendation G9:** The double blind can be lifted for fraud management purposes where one of three key conditions are met: **1)** Where information needs to be obtained from participants in the digital identity system to investigate suspected fraud or to assist with enforcement; **2)** Where information regarding a known fraud needs to be shared with other digital identity system participants; or **3)** Where the digital identity system is subject to a cyber-security incident that cannot be managed without lifting the double blind.	**Agree** The existing fraud management framework, as well as the proposed Data Sharing Framework (DSF), both incorporate this recommendation. The DSF is currently the subject of a PIA to ensure that privacy considerations are adequately considered in its development. Once the findings of those two PIAs are delivered, we will continue to work on the framework, including assessing whether the 3 criteria in this recommendation are appropriate.

Component / APP	Galexia Recommendation	DTA Response (25 October 2021)
Double blind	**Recommendation G10:** The double blind should not be lifted for the following purposes: **1)** To automatically check all identities or all transactions against specific criteria (e.g., checking across the entire ecosystem against a central list of safe or compromised identities or other particulars); or **2)** To profile the behaviour of individuals.	**Agree** The Trusted Digital Identity Bill contains: • a prohibition on profiling • a prohibition on one-to-many matching in relation to biometric information These rules apply regardless of whether a technical blind is in place, providing a greater level of protection. The proposed Data Sharing Framework incorporates this recommendation.
H. Data Retention Periods: A policy decision on data retention periods (and processes) for key data sets.		
	Recommendation H1: The DTA should develop a formal policy position with strict time limits for the retention of TDIF transaction data related to an individual's transactions in the Exchange. This could include a formal Records Authority. The policy position should explicitly restrict the retention of data to purposes required for digital identity services.	**Agree** The Trusted Digital Identity Bill contains rules on record keeping, including maximum retention periods for records for onboarded and offboarded entities. Additional rules have been added to restrict the sending of digital identity information outside Australia.

3. Ongoing consideration of privacy and updates to the TDIF

Galexia has observed the DTA make an ongoing and increased investment in its commitment to understanding and enhancing privacy across the digital identity ecosystem and this approach is to be commended.

The DTA is implementing a legislative framework and Galexia is strongly supportive of these activities and recognises a lot of the issues raised and recommendations made in PIAs 1, 2 and 3 may be addressed in this process. It is important to continue to be aware of prior recommendations and related privacy commitments. Refer to Appendix 4 – Initial and Second PIA Recommendation Summary.

Please note that this PIA continues the numbering of recommendations from PIA1 and PIA2 – and hence the first recommendation in this PIA starts at Recommendation 32.

Recommendation 32: Continue to consider recommendations from prior PIAs when making changes to the TDIF and implementing aspects of the digital identity ecosystem that may impact upon privacy

The findings and recommendations from all of the PIAs can be seen as a package. Privacy risks identified in each of the PIAs should be monitored to ensure that they are being addressed on a continuous basis. Subsequent review of privacy issues and PIAs should not need to make these recommendations again. Continue to maintain traceability and consider public commitments to recommendation responses and publish any changes.

Specific consideration of the proposed Digital Identity Legislation and the November 2020 Consultation Paper <www.digitalidentity.gov.au/have-your-say> is not within the scope of this PIA. This PIA does not consider the scope of the proposed legislation but recognises that the content of the legislation and related policy position may address recommendations made in this PIA.

4. Updates to the Privacy Requirements from TDIF3 to TDIF4

PIA2 (2018) considered the September 2018 version of Release 3 of the TDIF. Following this, after a period of internal review and external stakeholder consultation, Release 4 of TDIF was published in April 2020.[5]

This PIA considers changes to the TDIF Privacy Requirements between Release 3 and 4 – and specifically to the Privacy Requirements in Section 3 of *TDIF4 04 Functional Requirements*.

Appendix 2 contains a detailed mapping of the changes in TDIF4. It also briefly analyses the impact of the changes on privacy issues and identifies those that are weaker and stronger than the requirements in TDIF3. We have not undertaken a comprehensive analysis of changes in other sections or requirements documents.

Recommendation 33: Document changes to the TDIF and consider and communicate possible privacy impacts

To support openness and transparency it is important to continue to engage with stakeholders about proposed updates and identify and explain the impacts of both individual changes and also the sum of those changes. Consideration of privacy may extend beyond the Privacy Requirements section in the TDIF.

There are a number of changes from TDIF3 to TDIF4 that should be documented and explained to participants and stakeholders. There may be drafting irregularities or unintentional changes. We believe that TDIF4 would benefit from published responses from DTA about some of the key changes and the extent to which there have been changes to the TDIF privacy posture. This PIA should assist this.

Refer to Appendix 2 – Trusted Digital Identity Framework (TDIF) Policies and Standards – Privacy Requirements updates from TDIF3 (March 2019) to TDIF4 (March 2020).

[5] Digital Transformation Agency, *The Trusted Digital Identity Framework (TDIF) Documents* (Release 4, April 2020) <www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework/framework-documents>.

5. Eight Key Implementation Issues considered in this PIA

The privacy impacts of eight key issues and the proposed approach are considered in this PIA. The identification and wording for these issues were developed in consultation with DTA (and containing insight from privacy issues briefing notes developed in 2019/2020). Each issue was circulated to stakeholders for comment in June-September 2020.

- **A. Enduring Consent: A proposal to allow Users to provide enduring consent to the sharing of core data**

- **B. User Managed Digital Identity:** A proposal to facilitate User management of their Digital Identity

- **C. Deduplication:** A technical solution to facilitate identity resolution

- **D. Restricted Attributes:** A policy solution to establish a process for Relying Parties to seek additional and restricted attributes

- **E. Biometrics:** Proposal to manage the use and retention of biometric data presented during proofing

- **F. Governance Oversight:** A staged approach to the management of key privacy issues via governance and oversight mechanisms

- **G. Fraud Management**: A policy and technical proposal to enhance the fraud management function in Stage 1 of the Digital Identity system

- **H. Data Retention Periods:** A policy decision on data retention periods (and processes) for key data sets

Each of the eight key implementation issues and related APP/TDIF components raises slightly different privacy issues. The PIA follows the Commonwealth PIA Guidelines, so each section examines compliance against a specific APP.

A. Enduring Consent: A proposal to allow Users to provide enduring consent to the sharing of core data

A1. Proposal Overview: To allow Users to opt in to providing enduring consent

DTA proposes to allow Users to provide enduring consent for the sharing of their details with a Relying Party. Users will be asked to tick a box against the following wording:

> *Do you want us to remember your consent to share these details from <Identity Provider> with <Relying Party>?*

If the User does not tick the box, they will be prompted, every time they use the service, to consent to their details being shared again.

However, the enduring consent will not work in every circumstance:

1) The consent only applies to a single service, or services with the same Relying Party link;
2) If any additional attributes are sought by the Relying Party, then the enduring consent does not apply; and
3) If the attributes change via change of name or contact detail, the new attributes will display, and a new User consent will be required.

A2. Solution Overview: To allow Users to withdraw consent at any time

To manage this issue DTA is proposing to incorporate the following features:

1) Providing enduring consent will be entirely voluntary and opt-in;
2) A simple process will be available for withdrawing enduring consent; and
3) Plain, unambiguous language will be used.

A3. Enduring Consent: Findings and Recommendations Summary

Requirement	Galexia Finding	Galexia Recommendation	Status
APP 1: Open and Transparent Management of Personal Information	The APP 1 'equivalent' in the TDIF Privacy Requirements is Section 3.2.2 (Privacy Policy) of *TDIF4 04 Functional Requirements* – although some other sections also cover broader issues of openness (such as the sections on privacy governance). *Section 3.2.2* mandates that participants publish a privacy policy containing key information. Openness and transparency regarding enduring consent will rely on a mix of information in the privacy policy and the privacy notice (refer to APP 5 below). Existing relevant privacy policies will already cover the general concept of consent, but may need to be updated to include information on how to withdraw any enduring consent that has been provided.	**Recommendation A1: Relevant TDIF Participants (Identity Exchange) will need to update privacy policies to describe the process for withdrawing enduring consent.**	Action Required
APP 2: Anonymity and Pseudonymity	Not applicable – The TDIF is an identity framework designed to cater for transactions that require Level 2 and Level 3 identity. There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level.		-

APP 3: Collection of solicited personal information	Both APP 3 and its equivalent in section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* contain rules on the collection of personal information and data minimisation. The data minimisation requirement should be satisfied by the optional nature of enduring consent – an individual is choosing where to strike the balance between data collection and user convenience. Some additional data minimisation steps are form part of the design: ● Enduring consent only applies to a single service, or services with the same Relying Party link; ● If any additional attributes are sought by the Relying Party, then the enduring consent does not apply; and ● If the attributes change via change of name or contact detail, the new attributes will display, and a new User consent will be required. The design of the system (including features such as the Double Blind – discussed in section G4.B below) also means that the two consent mechanisms (individual and enduring) look the same to Relying Parties. Only the Exchange is aware whether a person is providing enduring consent – there is no flag shared across the entire Ecosystem. This is a privacy positive aspect of the proposal. Overall, as long as enduring consent is based on an explicit selection by individuals, the proposed change will be compliant with APP 3.		**Compliant**
APP 4: Dealing with unsolicited personal information	Not applicable		**–**
APP 5: Notification	APP 5 sets out requirements for the notice to be given to applicants. These requirements are mirrored and slightly enhanced in section 3.5 (Notification of Collection) of the *TDIF4 04 Functional Requirements*. The privacy notice will play a key role in managing enduring consent. This PIA is assessing the broad concept of enduring consent, rather than a specific proposal or draft privacy notice. One of the stakeholders made the suggestion to be more explicit about what was being consented to and suggested the following wording If you select this option, you won't have to provide your consent for us to share your details each time you access this service A few stakeholders made the common suggestion that users should be informed whenever their enduring consent is used and also suggested the process for withdrawing consent should accompany this statement. Stakeholders also pointed out that it is important to communicate the advantages/benefits to users – and the notices may be a sensible place to do this, but this is not a strict legal requirement.	**Recommendation A2: Update notices for relevant TDIF Participants (Identity Exchange) to support enduring consent.** The key requirements for the privacy notices include: – Use of plain, clear language; – Clarification that enduring consent is optional; – Information on the consequences of granting / not granting enduring consent; and – Information on the ability (and process) for withdrawing enduring consent at any time.	**Action Required**
APP 6: Use or Disclosure	APP 6 places restrictions on the use and disclosure of personal information. The Privacy Requirements in *TDIF4 04 Functional Requirements* place numerous additional restrictions on the use and disclosure of personal information: ● 3.6 Collection and use limitation ● 3.7 Limitation on use of behavioural information ● 3.8 Collection and disclosure of biometrics ● 3.9 Consent Overall, the provision of an enduring consent option should enhance compliance with APP 6 and the equivalent TDIF privacy requirements, as it gives individuals some more fine-grained control over the use and disclosure of personal information that they have previously submitted.		**Compliant**
APP 7: Direct Marketing	Not applicable – Section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* prohibits direct marketing		**–**
APP 8: Cross Border Disclosure	Not applicable.		**–**

APP 9: Government Related Identifiers	APP 9 places some restrictions on the use of government related identifiers by organisations. These requirements might potentially apply to some private sector IdPs and Relying Parties. However, APP 9 includes an important exception: *An organisation may use or disclose the government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a)).* Section 3.11 (Government Identifiers) of the Privacy Requirements in *TDIF4 04 Functional Requirements* (March 2020) also include a specific restriction on government related identifiers: *An Applicant MUST NOT create a new government identifier that is used across the identity federation (i.e., an identifier that is sent to more than one Relying Party or Identity Service Provider).* The TDIF requirement is stricter than APP 9 and has been included in order to prevent the development of a national identifier (either deliberately or accidentally). The provision of an enduring consent option should not have a significant impact on the use of Government Related Identifiers in the Digital Identity ecosystem. Individuals who opt to provide enduring consent will not be providing any more identifiers than those who provide consent for individual transactions.		**Compliant**
APP 10: Quality of Personal Information	APP 10 requires agencies to ensure that data is accurate and up to date in relation to the purpose for which it is collected and used. While section 3.13 (Quality of personal information) of the Privacy Requirements in *TDIF4 04 Functional Requirements* has some additional requirements for IDPs, these do not all apply to the Exchange. The provision of an enduring consent option should not have a significant impact on data quality in the Digital Identity ecosystem.		**Compliant**
APP 11: Security	APP 11 sets a somewhat vague standard for ensuring security of personal information. The TDIF contains a range of more specific security requirements and security audit requirements, in Section 4 (Protective Security Requirements) and Section7 (Functional Assessments) of *TDIF4 04 Functional Requirements (March 2020)* and references to security considerations in other key sections of the TDIF documentation. APP 11 states that security measures should be in proportion to the risk of the information being disclosed. Security requirements for enduring consent are covered by existing security arrangements for general consent (e.g., security audits, assessments etc.). We have not identified specific security issues raised by the enduring consent proposal itself.		**Compliant**
APP 12: Access	Section 3.12.1 (Access) in *TDIF4 04 Functional Requirements* addresses some of the limitations in APP 12, requiring all participants to meet higher access standards and enabling a more consistent experience for users. The provision of an enduring consent option should not have a significant impact on access rights in the Digital Identity ecosystem. One possible enhancement would be the provision of access to simple information on whether a user had provided or withdrawn enduring consent. This could potentially be managed via the proposed User Management Interface (refer to B. User Managed Digital Identity) rather than via Privacy Act access rights under APP 12.		**Compliant**
APP 13: Correction	Sections 3.12.2 (Correction) and 3.14 (Handling Privacy Complaints) in *TDIF4 04 Functional Requirements* (March 2020) contains additional requirements to APP 13, establishing a higher standard of corrections and complaints that TDIF participants must comply with. The provision of an enduring consent option should not have a significant impact on correction rights in the Digital Identity ecosystem.		**Compliant**

A4. Enduring Consent: Overall Findings

Overall the provision of enduring consent will be seen by many users as an enhancement – simplifying a complex process.

From a privacy compliance perspective, the proposal should be able to comply with the APPs and the TDIF privacy requirements – as long as the privacy notice is clear, and the system includes a simple mechanism for withdrawing enduring consent at any time. The proposal also places a significant emphasis on data minimisation – and this adds to the privacy **positive** impact of the proposal.

Whilst stakeholders held concerns about the proposal there is general support for the solution – and this is strongly conditional upon all the aspects of the proposed approach being implemented and that the ‘opt-out’ method was simple and easy and that this was independently tested.

Galexia notes that this PIA is assessing the concept and not a detailed technical proposal or draft privacy notice.

B. User Managed Digital Identity: A proposal to facilitate User management of their Digital Identity

B1. Proposal Overview: To introduce tools to facilitate User management of Digital Identity

DTA is proposing to introduce tools to help Users monitor and manage their own Digital Identity. Specifically, the DTA is considering how tools can be incorporated in the Digital Identity system that will help Users see a history of their key transactions. DTA recognises that there is a need for an Individual History Log functionality, so that Users can check recent transactions (e.g., for suspicious activity). However, the provision of this service will need to be balanced against other privacy risks.

B2. Solution: To encourage participants to provide User management tools for devices and to mandate an Individual History Log interface at the Identity Exchange

To manage this issue, DTA is proposing an **Individual History Log Interface** – this service will be mandatory and will be provided by the Identity Exchange. It may be limited to recent transactions or a smaller number of transactions in order to achieve the right balance between transparency and privacy.

B3. TDIF requirements for the Identity Exchange and the User Dashboard and Consumer History

TDIF4: 04 Functional Requirements (March 2020 v1.0)

> 3.12 Access, correction and individual history log
>
> 3.12.3 Individual history log
>
> The *Applicant* MUST provide *Individuals* with a centralised view of the metadata of services the *Individual* accessed, the time of access and the *Attributes* passed to the Relying Party unless such information has already been destroyed by the *Applicant* in accordance with the TDIF.

As noted in the TDIF requirements above, the availability of the transaction history may be time limited in order to reduce overall privacy and security risks.

TDIF4 TDIF Glossary (March 2020 v1.0)

> **Consumer History.** The history of all a User's interactions with an *Identity Exchange*.
>
> **User Dashboard.** A collective term for the feature that an *Identity Exchange* provides for a User to view their consumer history and manage their interactions with the *Australian Government's identity federation*.

TDIF4 TDIF 06A Federation Onboarding Guidance (March 2020 v1.0)

> **4.1.2 Audit History, Consumer History and User Dashboard**
>
> The *User Dashboard* is a collective term for the features that an *Identity Exchange* provides to a *User* that has been *Authenticated* by a *Credential Service Provider*. This includes:
>
> - Access to the *Consumer History*, which is the history of all the *User's* interactions performed via an *Identity Exchange* using the *Identity Service Provider* they are using to access the *User Dashboard*.
> - Ability to revoke ongoing *Consent* to shared *Attributes* with a *Relying Party*.
>
> The audit history is a historical record of all federated identity interactions that relate to a *Digital Identity*. This includes any requests and responses between:
>
> - A *Relying Party* and an *Identity Exchange*.
> - An *Identity Service Provider* and an *Identity Exchange*.
> - An *Attribute Service Provider* and an *Identity Exchange*.

The audit history includes:

- Timestamp.
- Interaction Type. E.g., *OIDC Authentication Request*.
- Audit ID. The *Identity Exchange* will need to be able to correlate the requests and responses in an interaction.
- Entity. An *Identity Service Provider*, *Attribute Service Provider* or a *Relying Party*.
- Entity Link. Any *identity* link used in the interaction, such as the *RP Link* or I*dP Link*.
- Names of any Attributes requested or returned.
- Any level of assurance requested or returned.

No identity attribute values are stored in the audit history.

The information available to be viewed about a transaction at the *User Dashboard* includes:

- The attributes requested by a *Relying Party*.
- *Consent* provided.
- *Attributes* returned to a *Relying Party* (but not the actual values returned).

The *User* will need to be *Authenticated* by an *Identity Service Provider* to access the *User Dashboard*.

TDIF4 TDIF 06 Federation Onboarding Requirements (March 2020 v1.0)

4.1.2 Audit history, consumer history and user dashboard

TDIF Req: FED-04-01-06; Updated: Mar-20; Applicability: X
The *Applicant* MUST provide a method for a *User* to view their *Consumer History* and manage their *Consent*.

TDIF Req: FED-04-01-07; Updated: Mar-20; Applicability: X
The *Applicant* MUST include in the user's *Consumer History* the history of all the interactions the user has performed via the *Identity Exchange* using the *Identity Service* Provider and enable the user to view the consent they have provided to share attributes provided by either an *Attribute Service Provider* or an *Identity Service Provider* with a *Relying Party*.

TDIF Req: FED-04-01-08; Updated: Mar-20; Applicability: X
The *Applicant* MUST ensure that the *User Dashboard* feature does not store personal *Attributes* of the User beyond the *User's* presence at the *User Dashboard*.

B4. User Managed Digital Identity: Findings and Recommendations Summary

Requirement	Galexia Finding	Galexia Recommendation	Status
APP 1: Open and Transparent Management of Personal Information	The APP 1 'equivalent' in the TDIF Privacy Requirement is *section 3.2.2 (Privacy Policy)* of *TDIF4 04 Functional Requirements* – although some other sections also cover broader issues of openness (such as the sections on privacy governance). *Section 3.2.2* mandates that participants publish a privacy policy containing key information. This requirement raises issues around the development of the Individual History Log functionality. ● **Issue 1:** Accredited TDIF entities (the Exchange) need to be open about what they are doing – i.e., that there is an individual History Log and the nature of information collected and used for this purpose.	**Recommendation B1: Develop and publish clear documentation of the proposed Individual History Log functionality** There may need to be multiple versions, including: – technical documentation for implementing participants (the Exchange) – clear and easy-to-understand explanation to individuals, including articulation of benefits and protections.	**Action Required**
APP 1: Open and Transparent Management of Personal Information	● **Issue 2:** Accredited TDIF entities must not mislead the public in any way, and the implementation of the Individual History Log functionality will need to be checked against all of the other privacy promises that have been made to consumers (e.g., statements about the double blind, prohibitions on user profiling, etc).	**Recommendation B2: Review relevant public facing Accredited TDIF participant privacy policies and notices for changes required due to the introduction of the Individual History Log functionality** In order to ensure that consumers are not misled by existing statements, review any relevant public facing Accredited TDIF participant privacy policies and notices to ensure that existing statements or promises on information collection, use and disclosure do not require amendment following the introduction of Individual History Log functionality.	**Action Required**
APP 2: Anonymity and Pseudonymity	Not applicable – The TDIF is an identity framework designed to cater for transactions that require Level 2 and Level 3 identity. There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level.		**–**
APP 3: Collection of solicited personal information	Both APP 3 and its equivalent in section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* contain rules on the collection of personal information and data minimisation. The provision of an individual History Log functionality should not have a significant impact on the collection of personal information in the Digital Identity ecosystem. The proposal has an impact on the management and presentation of information, but does not require the collection of any additional information. In relation to the data minimisation requirement, the information available via the Interface may be limited (e.g., to recent transactions or a smaller number of transactions) in order to achieve the right balance between transparency and privacy At this early stage of the proposal no specific limit has been set, and this issue may require further user testing and analysis of overall usage patterns in order to strike the right balance. Refer to Recommendation B4.		**Compliant**
APP 4: Dealing with unsolicited personal information	Not applicable		–

APP 5: Notification	APP 5 sets out requirements for the notice to be given to applicants. These requirements are mirrored and slightly enhanced in section 3.5 (Notification of Collection) of the *TDIF4 04 Functional Requirements*. The provision of an individual History Log functionality should not have a significant impact on privacy notices. Privacy notices may potentially mention the Interface as a benefit for users, but this is not a strict legal requirement.		**Compliant**
APP 6: Use or Disclosure	APP 6 places restrictions on the use and disclosure of personal information. The Privacy Requirements in *TDIF4 04 Functional Requirements* place numerous additional restrictions on the use and disclosure of personal information: ● 3.6 Collection and use limitation ● 3.7 Limitation on use of behavioural information ● 3.8 Collection and disclosure of biometrics ● 3.9 Consent The provision of an individual History Log functionality is a new use of the personal information in the Digital Identity system. This use is for the benefit of the consumer and is a permissible use under the APPs and the TDIF. However, it may be an ‘unexpected’ use if Privacy policies are not updated or if this use contradicts with previous assurances made to consumers on the availability of their transaction histories (see the discussion under APP 1). The proposal does not envisage any additional disclosure of information other than directly to the individual themselves. Overall, the proposal appears to comply with APP 6 and the TDIF Privacy Requirements.		**Compliant**
APP 7: Direct Marketing	Not applicable – Section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* prohibits direct marketing.		**–**
APP 8: Cross Border Disclosure	Not applicable.		**–**
APP 9: Government Related Identifiers	Not applicable.		**–**
APP 10: Quality of Personal Information	APP 10 requires agencies to ensure that data is accurate and up to date in relation to the purpose for which it is collected and used. While section 3.13 (Quality of personal information) of the Privacy Requirements in *TDIF4 04 Functional Requirements* has some additional requirements for IDPs, these do not all apply to the Exchange. The provision of an individual History Log functionality should enhance data quality. Individuals will be able to review recent transactions, and challenge suspicious transactions, leading to the detection and investigation of fraud and errors.		**Compliant**

APP 11: Security	APP 11 sets a somewhat vague standard for ensuring security of personal information. The TDIF contains a range of more specific security requirements and security audit requirements, in Section 4 (Protective Security Requirements) and Section7 (Functional Assessments) of *TDIF4 04 Functional Requirements (March 2020)* and references to security considerations in other key sections of the TDIF documentation. APP 11 states that security measures should be in proportion to the risk of the information being disclosed. Managing security will be crucial for the Individual History Log functionality. Such portals are typically security weak points or targets. A good example of a similar concept that is the subject of regular security attacks is the provision of user access to credit reports. The portal can expect to be the subject of impersonation attacks and will need to set very high standards for access and monitoring. This is a significant concern of stakeholders. The proposal must include the ability to quickly **suspend** access to the portal, as well as the full suite of typical security controls (access logging, security audits etc.) From a security perspective, it may be appropriate to introduce the Interface to a small number of accounts in a series of security trials, rather than introducing the Interface for all accounts at the same time. The security requirements in APP 11 and the TDIF also include requirements related to data retention. The exact amount of data that will be available via the Interface has not yet been determined. From a security perspective, the data should be limited (e.g., to recent transactions or to a maximum number of transactions). This will help the Interface avoid becoming a complete user profile or a high value security target.	**Recommendation B3: The Individual History Log functionality should be the subject of a detailed security assessment and strict security measures that reflect the high likelihood of attacks against this mechanism.** **Recommendation B4: Develop the data retention policy requirements to be applied to the Centralised User Management Interface to provide access to recent transactions or a maximum number of transactions.** The exact number can be set following security assessments and user trials.	**Action Required**
APP 12: Access	Section 3.12.1 (Access) in *TDIF4 04 Functional Requirements* addresses some of the limitations in APP 12, requiring all participants to meet higher access standards and enabling a more consistent experience for users. The provision of an individual History Log functionality should enhance user access to data, in a way that complements typical access rights under APP 12. Individuals will be able to review recent transactions and get a clear view of the information that has been collected about them.		**Compliant**
APP 13: Correction	Sections 3.12.2 (Correction) and 3.14 (Handling Privacy Complaints) in *TDIF4 04 Functional Requirements* (March 2020) contains additional requirements to APP 13, establishing a higher standard of corrections and complaints that TDIF participants must comply with. The provision of an individual History Log functionality should enhance correction rights. Individuals will be able to review recent transactions, and challenge suspicious transactions, leading to the detection and investigation of fraud and errors.		**Compliant**

B5. User Managed Digital Identity: Overall Findings

Overall, the provision of an individual History Log functionality will bring some benefits, including improvements to data quality and simplifying user's access to their own data.

From a privacy compliance perspective, the proposal should be able to comply with the APPs and the TDIF privacy requirements, with some updates to relevant privacy policies and strengthening of security arrangements.

A key issue that is still to be determined is how much data will be available via the Interface. This PIA recommends placing a limit on the data (e.g., only recent transactions or a specific maximum number of transactions). However, at this early stage of development it is difficult to set an exact limit. More user testing, security reviews and data analysis will be required in order to get the right balance between privacy, security and transparency.

Whilst stakeholders held some concerns about the proposal there is general support for improvements to transparency in the system.

C. Deduplication: A technical solution to facilitate identity resolution

C1. Proposal Overview: To allow the Identity Exchange to reconcile duplicates when the same User uses a different Digital Identity to seek services at a Relying Party

Users are allowed to obtain a Digital Identity from more than one Identity Provider, and they are free to use any of these Digital Identities when accessing Government services. DTA is proposing to allow the Identity Exchange to reconcile duplicates when the same User uses a different Digital Identity to seek services at a Relying Party.

To do this, the Identity Exchange will maintain a key of any Relying Party links to individuals, including a hash of one Commencement of Identity (CoI) document number (e.g., a passport number). If a key containing the same CoI document number already exists it will trigger a reconciliation process and the Relying Party will know that the person presenting is a duplicate.

C2. Solution Overview: That the mapping process and keys can only be used for the purpose of reducing duplicates, and that the use of the key for any other purposes will be prohibited

To manage this issue DTA is proposing that the mapping process and keys can only be used for the purpose of reducing duplicates, and that the use of the key for any other purposes will be prohibited (e.g., wider surveillance).

The deduplication process will identify the majority of duplicates, but not 100%.

Note: As at October 2021, Deduplication is currently not operational in the Australian Government Digital Identity System. This PIA considered deduplication only to canvass potential privacy issues with a possible solution. It is currently under consideration as a possible solution.

C3. TDIF Requirements for Deduplication

The current TDIF requirements for Deduplication (applying to Identity Providers and the Identity Exchange, with varying requirements) are:

> *TDIF4 TDIF Glossary* (March 2020 v1.0)
>
> > **Deduplication.** The process of determining whether two or more *Digital Identity* records relate to the same *Individual* or a different *Individual*, whether within a single IDP (IDP deduplication), or across multiple IDPs, at the *Identity Exchange* (ecosystem deduplication).
>
> *TDIF4 06D Attribute Profile* (March 2020 v1.0)
>
> > **3. Core Attribute Profile**
> >
> > **3.2. IdP Specific Attribute**
> >
> > This section refers to attributes which the *IdPs* are required to be able to share if requested by the *Identity Exchange*, but the *Identity Exchange* is not required to share.
> >
> > **Table 12:** IDP specific attributes.

Attribute	Description	Mandatory/ Optional
TDIF EDI	Evanescent Deterministic Identifier used by an exchange for the purposes of Deduplication.	Mandatory

TDIF4 06A Federation Onboarding Guidance (March 2020 v1.0)

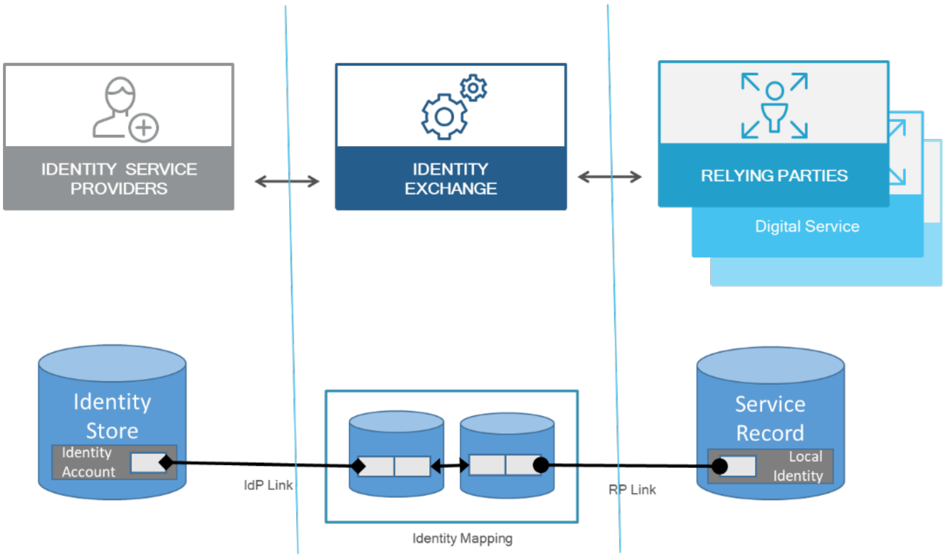
2.2. Feature-Specific Technical Integration Requirements

2.2.1 Identity Resolution

Identity resolution refers to the process of determining whether multiple records relate to the same person or a different person, including *Digital Identity* records at one or more *Identity Service Providers* and/or *Identity Exchange's*, and/or agency records at a *Relying Party*. An *Identity Exchange* utilises *Pairwise Identifiers* and *Deduplication* to conduct identity resolution. It is also expected that *Relying Parties* will have their own identity resolution processes to avoid duplicate accounts, if avoiding this situation is important for that particular *Relying Party*.

2.2.1.1. Pairwise Identifiers

Figure 5: Identity Linkages in the TDIF identity federation.



The identity links in the *Identity Federation* are used to support the *Authentication* processes that enable an *Individual* to have ongoing access to digital services at a *Relying Party*.

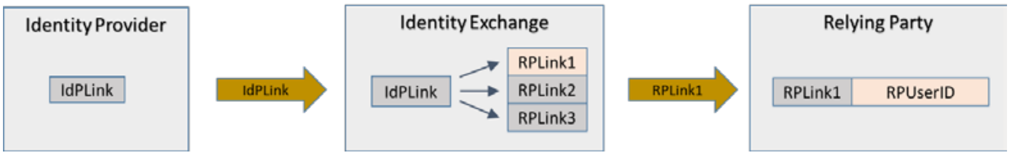
To enable *Users* to *Authenticate* and then be able to reuse their *Identity* at a *Relying Party*, the following identity linkages exist as persistent pseudonymous identifiers in the *Identity Federation*:

- *IdP Link*. This identifier links the identity for an authenticated user at an IDP with the digital identity brokered by an Identity Exchange. This identifier is generated by the Identity Service Provider.
- *RP Link*. This identifier links the digital identity brokered by an Identity Exchange to the service record (client record, customer record) at a Relying Party. The Identity Exchange generates this identifier. This RP Link is unique for each user at each Relying Party.

Both the *IdP Link* and *RP Link* are implemented using *Pairwise Identifiers*. An *Identity Exchange* maintains a mapping between the *IdP Link* (the identity at an Identity Service Provider) and the *RP Link* (the service record at the Relying Party).

When a user authenticates to a *Relying Party* using the services of an *Identity Service Provider* the same *RP Link* will be presented to the *Relying Party* across all authentication events.

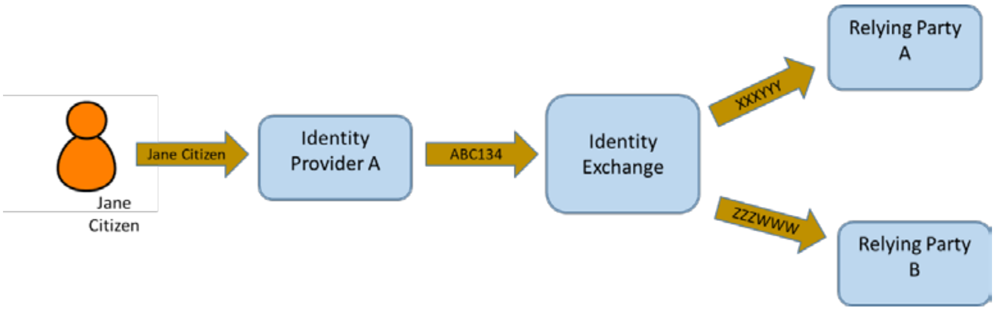
Figure 6: Identity Mapping across any Identity Exchange.



1. The *Identity Service Provider* persists a single identifier for each unique identity it recognises (*IdP Link*).
2. At the time of *Authentication*, the *IdP Link* is passed to the *Identity Exchange*.
3. The *Identity Exchange* persists the *IdP Link* against a table of internally generated *Relying Party* specific identifiers (*RP Link*).
4. The *Identity Exchange* selects or generates the *RP Link* that matches the *Relying Party* that has requested *Authentication*.
5. The *Identity Exchange* passes the *RP Link* to the *Relying Party*.
6. The *Relying Party* maps the *RP Link* to its internal customer record.

An example of identity mapping that occurs in the *Authentication* of a *User* is shown below:

***Figure 7**: Mapping of a User's identity in an Authentication Event.*



The requirements in section 2.2.1.1 of the *TDIF: 06 Federation Onboarding Requirements* describe the implementation of these *Pairwise Identifiers*.

The use of *Pairwise Identifiers* is a key privacy mechanism. When a *Relying Party* utilises them they should consider specific privacy and administrative arrangements that operate in their jurisdiction, including any legislative requirements concerning how personal information should be collected, accessed and stored correctly.

2.2.1.1.1. OIDC Relying Party Sector Identifiers

The *OIDC* specification closely couples the concept of a *Relying Party* to a client, or a software application instance. A *TDIF Relying Party* may need to register multiple *OIDC* clients for the different digital services that it provides but still require the same underlying *Pairwise Identifier* for an authenticated *User* to be passed to all of its registered *OIDC* clients.

The *OIDC* standard provides a mechanism to enable multiple clients to receive the same *Pairwise Identifier*. This mechanism is termed a Sector Identifier and is defined in the **[OpenID.Core]** <openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg> and is further expanded on the specification for Dynamic Client Registration <openid.net/specs/openid-connect-registration-1_0.html#SectorIdentifierValidation>.

2.2.1.2. Deduplication

The aim of *Deduplication* is for *Individuals* with multiple *Digital Identities* at one or more *IdPs* to appear as having a single *Digital Identity* to a *Relying Party*. In the *Identity Federation*, this is conducted by the *Identity Exchange* with assistance from *Identity Service Providers*, who provide an *EDI* which an *Identity Exchange* may use for the purposes of *Deduplication*.

Deduplication in the system relies on *Identity Service Providers* passing a unique attribute called an Evanescent Deterministic Identifier (*EDI*) in response to an *Authentication Request* for a User. When generating an *EDI*, the *IdP* is required to combine several *Attributes* taken from verified documents, concatenate these, convert the resulting string to utf-8 and then hash the text using SHA-256. The document type code which is required to be used in this transaction is the same document type code as is used to request the document. This can be found in section 6.1 of the *TDIF: 06D – Attribute Profile*.

The document used to generate an EDI is specified in section 2.2.1.2 of the *TDIF: 06 – Federation Onboarding Requirements*. These documents and the precedence of documents to be used will be updated by the DTA as more documents become accessible in the federation. Furthermore, for new documents, the DTA will advise what attributes need to be used and in what order these will be used.

An *Identity Exchange* then utilises the *EDI* to deduplicate identities. They are not allowed to store the *EDI*, or send it to other *Participants* in the *Identity Federation*.

One implementation of *Deduplication* is to transform the *EDI* into a unique identifier specific for a *User* at each *Relying Party*. This is then used as a lookup to check whether a different *Digital Identity* with the same unique identifier has previously accessed that *Relying Party*.

If there is, the *RP link* of that *Digital Identity* is mapped to the *IdP link* of the *User*. This ensures that *Deduplication* isn't done across entire identities, but instead is done at each *Relying Party* and that an *Individual* can appear the same to a *Relying Party*, regardless of which *IdP* was used. This unique identifier can also be configured in accordance with *Relying Party* sector identifiers.

TDIF4 06 Federation Onboarding Requirements (March 2020 v1.0)

2.3 Feature-specific technical integration requirements

The section sets out the technical integration requirements for specific features of the Identity Federation

2.3.1 Identity resolution

…

2.3.1.2 Deduplication

TDIF Req: FED-02-03-10; **Updated:** Mar-20; **Applicability:** X
The Applicant MUST have a process to conduct Deduplication of identities which pass through an Identity Exchange to ensure that a User with multiple digital identities is presented as the same user to a Relying Party.

TDIF Req: FED-02-03-11; **Updated:** Mar-20; **Applicability:** X
The Applicant MUST only deduplicate identities which have been proved to the same Identity Proofing Level.

TDIF Req: FED-02-03-12 **Updated:** Mar-20; **Applicability: I**
If the TDIF EDI attribute is requested by an Identity Exchange, the Applicant MUST return an EDI constructed using the document specified in Table 1 (as updated by DTA from time to time) according to the Identity Proofing Level used in the authentication context.

TDIF Req: FED-02-03-13 **Updated:** Mar-20; **Applicability: I**
The Applicant MUST return an EDI constructed using only such documents specified in Table 1 (as updated by DTA from time to time) as are bound to the current authentication context.

TDIF Req: FED-02-03-14 **Updated:** Mar-20; **Applicability: I**
The Applicant MUST ensure that the documents and attributes used to construct an EDI reflect the most up to date documents and attributes bound to the current authentication context.

TDIF Req: FED-02-03-15; **Updated:** Mar-20; **Applicability:** I
When constructing an EDI using a document the Applicant MUST concatenate the document type code URN from section 6.1 of the TDIF: 06D – Attribute Profile and the attributes specified in Table 2 in the order specified in Table 2, for that document, using the attribute formats specified in Table 3.

TDIF Req: FED-02-03-15a **Updated:** Mar-20; **Applicability:** I
If the User has not verified any of the documents in Table 1 (as updated by DTA from time to time), the Applicant MUST construct an EDI by concatenating the IP Link for the User and a suitable globally-unique identifier for the Applicant (e.g., OIDC Issuer URI).

TDIF Req: FED-02-03-15b; **Updated:** Mar-20; **Applicability:** I
The string resulting from either TDIF Req FED-02-03-15 or TDIF Req FED-02-03-15a MUST then be encoded using UTF-8, before being hashed using the SHA-256 algorithm.

Table 1: Documents used to build an *EDI*

IP Level	Details
IP 1	The first available document from the following list: 1. Verified Email Address 2. Verified Mobile Number
IP 1 PLUS **IP 2** **IP 2 PLUS**	The first available document from the following list: 1. Birth Certificate 2. Citizenship Certificate 3. Visa 4. Passport 5. Driver Licence 6. ImmiCard 7. Medicare Card
IP 3	The first available document from the following list: 1. Birth Certificate 2. Citizenship Certificate 3. Visa 4. Passport
IP 4	The first available document from the following list: 1. Birth Certificate 2. Citizenship Certificate 3. Visa

Table 2: Document Attributes used to build an EDI

Document type	Specified Attributes
Passport	• Passport Number
NSW Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State
ACT Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State
NT Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State
QLD Birth Certificate	• Certificate Number if Available • Document Date of Birth • Document Issuer State • Registration Date
WA Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • State or Territory of Issue
SA Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State

TAS Birth Certificate	● Certificate Number if available, else use Registration number ● Document Date of Birth ● Document Issuer State ● Registration Date
VIC Birth Certificate	● Registration Number ● Document Date of Birth ● Document Issuer State
Citizenship Certificate	● Document Date of Birth ● Stock Number
Visa	● Document Date of Birth ● Foreign Passport Number
Driver Licence	● Licence Number ● Document Issuer State
Medicare Card	● Medicare Card Number ● Individual Reference Number ● Card Colour
ImmiCard	● ImmiCard Number

Table 3: Specified attribute data format

Attribute/sub-attribute	Type	Format	Maximum Length
Document Issuer State	String	Values are “NSW’, “QLD”, “VIC”, “TAS”, “WA”, “SA”, “ACT”, “NT”	3
Document Identifier	String	0 or more characters. This includes Certificate Number, Passport Number, Registration Number, Stock Number, Licence Number and Foreign Passport Number.	50
Document Date of Birth	String	ISO 8601:2004 format: YYYY-MM-DD. Note partial dates are also valid, i.e., YYYY, YYYY-MM	10
Registration Date	String	ISO 8601:2004 format: YYYY-MM-DD. Note partial dates are also valid, i.e., YYYY, YYYY-MM	10
Document Country of Issue	String	1 or more characters	50

TDIF Req: FED-02-03-16; **Updated:** Mar-20; **Applicability:** I
The Applicant MUST NOT provide access to an EDI to any party other than an Identity Exchange.

TDIF Req: FED-02-03-17; **Updated:** Mar-20; **Applicability:** X
The Applicant MUST NOT store an EDI received from an Identity Service Provider or use it as their Pairwise Identifier for the User being authenticated.

TDIF Req: FED-02-03-18; **Updated:** Mar-20; **Applicability:** X
The Applicant MUST NOT provide access to an EDI to any other party in the Identity Federation.

TDIF Req: FED-02-03-19; **Updated:** Mar-20; **Applicability:** X
If the Applicant uses the EDI to conduct Deduplication, it MUST NOT do so across the Identity Federation, but instead only conduct deduplication at a sector identifier level.

TDIF Req: FED-02-03-20; **Updated:** Mar-20; **Applicability:** X
The Applicant MAY request an EDI to conduct Deduplication as part of an authentication request made to an Identity Service Provider.

C4. Deduplication: Findings and Recommendations Summary

Requirement	Galexia Finding	Galexia Recommendation	Status
APP 1: Open and Transparent Management of Personal Information	The APP 1 'equivalent' in the TDIF Privacy Requirement is *section 3.2.2 (Privacy Policy)* of *TDIF4 04 Functional Requirements* – although some other sections also cover broader issues of openness (such as the sections on privacy governance). *Section 3.2.2* mandates that participants publish a privacy policy containing key information. This requirement presents a challenge for the deduplication solution. ● **Issue 1:** Accredited TDIF entities need to be open about what they are doing – i.e., that there is a deduplication capability and the nature of information collected and used for this purpose. Section 2.2.1 (Identity Resolution) in *TDIF4 06A Federation Onboarding Guidance* (March 2020) contains technical information. Consumer documentation is being prepared.	**Recommendation C1: Develop and publish clear documentation and guidance of the Identity Deduplication functionality** There may need to be multiple versions, including: – technical documentation for implementing participants – clear and easy-to-understand guidance to individuals, including articulation of benefits and protections.	**In Progress**
APP 1: Open and Transparent Management of Personal Information	● **Issue 2:** Accredited TDIF entities must not mislead the public in any way, and the new deduplication solution will need to be checked against all of the other privacy promises that have been made to consumers (e.g., statements about the double blind).	**Recommendation C2: Review relevant public facing Accredited TDIF participant privacy policies and notices** In order to ensure that consumers are not misled by existing statements, review any relevant public facing Accredited TDIF participant privacy policies and notices to ensure that existing statements or promises on information collection, use and disclosure do not require amendment following the introduction of deduplication.	**In Progress**
APP 2: Anonymity and Pseudonymity	Not applicable.		**–**
APP 3: Collection of solicited personal information	The deduplication solution does not present any new issues or challenges for compliance with APP 3 (Collection) and APP 3 and its TDIF equivalent – section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements.* The data is collected directly from the applicant and not from a third party. The data being collected is kept to the minimum reasonable required for identity verification purposes (as deduplication is a legitimate part of identity verification). Deduplication does not have a direct impact on consent arrangements under the TDIF. The overall approach is that most personal information will be collected by IdPs based on the provision of adequate notice (see APP 1 and APP 5). Some specific data collection will require explicit consent, but this is limited to biometric information.		**Compliant**
APP 4: Dealing with unsolicited personal information	Not applicable.		**–**

APP 5: Notification	APP 5 sets out requirements for the notice to be given to applicants. These requirements are mirrored and slightly enhanced in section 3.5 (Notification of Collection) of *TDIF4 04 Functional Requirements*. The deduplication solution does not require any new or expanded privacy notices. The key piece of personal information (a passport number or driver licence number) is already being provided in accordance with a privacy notice that complies with APP 5. However, compliance with APP 5 is heavily reliant on compliance with APP 1, in that the privacy notice usually directs Users to the privacy policy for more information. It is also important that IdP privacy notices are not misleading in any way, although the opportunity for a misleading statement in short privacy notices is limited (compared to more detailed privacy policies). Note: Galexia has briefly checked the Australia Post Digital ID[6] and ATO myGov Id documentation.[7] There do not appear to be any statements that require revision in order to avoid misleading Users about the deduplication solution. That is not to say that these documents could not be improved and clarified once deduplication is introduced.		**Compliant** (Note that this status relies heavily on addressing issues raised under APP 1 above)
APP 6: Use or Disclosure	APP 6 places restrictions on the use and disclosure of personal information. The Privacy Requirements in *TDIF4 04 Functional Requirements* place numerous additional restrictions on the use and disclosure of personal information: • 3.6 Collection and use limitation • 3.7 Limitation on use of behavioural information • 3.8 Collection and disclosure of biometrics • 3.9 Consent **Disclosure** In practice, the IdPs will only disclose deduplication data to the Identity Exchange, and the Exchange will not disclose this information to any third party. APP 6 allows the initial disclosure by the IdP, as identity verification is a primary purpose, and this would reasonably include the management of duplicates. **Use** The IdPs do not use the deduplication data at all. Relying Parties are not even aware of the deduplication data. The Identity Exchange does use the deduplication data, but only for the purpose of identifying and managing duplicates. Overall, the design of the deduplication solution does minimise disclosure and use of personal data as much as possible, while still allowing some duplicates to be identified and managed. In order to build trust and confidence in the system, the TDIF Privacy Requirements could be enhanced to include a direct reference to the deduplication data, and a section restricting the use and disclosure of this data.	**Recommendation C3: Update the TDIF to include a specific section on the deduplication data – including a list of permitted uses of the data and a list of prohibited uses.**	**Action Required**
APP 7: Direct Marketing	Not applicable – Section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* prohibits direct marketing		**–**
APP 8: Cross Border Disclosure	Not applicable.		**–**

[6] Australia Post, *Digital iD™ Privacy Notice* (13 August 2020) <digitalid.com/privacy.html> and repeated in Australia Post, *Digital iD™ Terms of Use* (13 July 2019) <digitalid.com/terms/web.html>.

[7] Australian Government, *myGovID Privacy Policy* (August 2019) <www.mygovid.gov.au/mygovid-privacy-policy>.

APP 9: Government Related Identifiers	APP 9 places some restrictions on the use of government related identifiers by organisations. These requirements might potentially apply to some private sector IdPs and Relying Parties. However, APP 9 includes an important exception: *An organisation may use or disclose the government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a)).* Section 3.11 (Government Identifiers) of the Privacy Requirements in *TDIF4 04 Functional Requirements* also include a specific restriction on government related identifiers: *An Applicant MUST NOT create a new government identifier that is used across the identity federation (i.e., an identifier that is sent to more than one Relying Party or Identity Service Provider).* The TDIF requirement is stricter than APP 9 and has been included in order to prevent the development of a national identifier (either deliberately or accidentally). In practice, the new identifier / digest that is for deduplication purposes is not sent to more than one TDIF participant, so it is not used 'across the federation'.[8]		**Compliant**
APP 10: Quality of Personal Information	APP 10 requires agencies to ensure that data is accurate and up to date in relation to the purpose for which it is collected and used. Section 3.13 (Quality of personal information) of the Privacy Requirements in *TDIF4 04 Functional Requirements* has some additional requirements for IDPs. The intention of the deduplication solution is to assist in the overall management of duplicate identities. It is not designed as a 100% guarantee of accuracy. The solution is also being delivered as a tool to enhance the user experience and convenience, especially at Relying Parties. It is not trying to eliminate duplication from a security or a risk perspective. Relying Parties may still experience some instances of duplicate users being presented via the Identity Exchange as different users. Relying Parties will need to have their own systems in place to manage this risk. However, in those cases where the Exchange detects a duplicate and presents this to the Relying Party as the same person, there is a very high degree of likelihood that this information is accurate. Some design factors may have an impact on data quality. For example, the current proposal envisages that a range of Commencement-of-Identity (CoI) documents may be used in the deduplication solution – including passports, visas, drivers licences and potentially birth certificates. Some of these CoI documents will present data quality challenges. For example, older driver licences and birth certificates may in some rare cases have the same number across states. The DTA TDIF team is aware of these issues and is considering a range of trials and evaluations to ensure an acceptable degree of accuracy.	**Recommendation C4: The deduplication solution should be subject to trials and evaluations to ensure an acceptable degree of data accuracy, prior to full implementation of the solution.**	**In Progress**

[8] Note that this PIA has assumed that there is only one Identity Exchange in the TDIF. Some additional issues may arise where more than one Identity Exchange is accredited under the TDIF and may require further consideration of privacy impacts.

APP 11: Security	APP 11 sets a somewhat vague standard for ensuring security of personal information. The TDIF contains a range of more specific security requirements and security audit requirements, in Section 4 (Protective Security Requirements) and Section7 (Functional Assessments) of *TDIF4 04 Functional Requirements (March 2020)* and references to security considerations in other key sections of the TDIF documentation. Privacy regulators and consumer stakeholders will have concerns that the process of hashing an existing identifier (such as a passport) will be insecure or vulnerable to reverse engineering. They will also be concerned that the resulting hash / digest or identifier itself may reveal some personal information. In practice, any person with knowledge of the original identifier (e.g., a passport number) and the hash process will be able to create the same identifier / digest as the one used in the deduplication process. APP 11 states that security measures should be in proportion to the risk of the information being disclosed. In this case, the risk of the new identifier / digest being exposed is minimal, as there is very little that can be done with this information. Nevertheless, the overall security of the deduplication solution should be tested against the TDIF security requirements. This testing should be independent.	**Recommendation C5: Include the deduplication solution in the high-level DTA security review of the TDIF environment.** **Recommendation C6: Add the deduplication solution to the security audit requirements for Accredited TDIF participants.**	**Action Required**
APP 12: Access	The deduplication solution does not raise new or specific concerns regarding access and compliance with APP 12. However, access to information held by the Identity Exchange is complicated in the TDIF – and it will be important to manage consumer expectations about what information is accessible. The Identity Exchange is required to offer consumers a simple and accessible Dashboard that will allow them to see recent transactions. This is an important step in managing potential fraud. Consumers should generally be able to see any transactions where deduplication has been utilised. Whether or not this is possible or reasonable in practice may require some further exploration.		**Compliant** (Further measures possible)
APP 13: Correction	Not applicable.		**–**
Governance: CoI Document Custodians	The deduplication solution may have an impact on two areas of privacy governance within the TDIF. **Issue 1: Commencement of Identity (CoI) Document Custodians** Many of the CoI documents are issued by State and Territory agencies. The use of these documents outside their original purpose, even where the new purpose is closely related to identity verification, should be done on a collaborative basis. For example, the Registrars of Births, Deaths and Marriages often have specific views on the use of their documents for identity verification, especially where the documents contain attributes such as sex, gender and change of name.[9]	**Recommendation C7: The DTA TDIF team should consult with State and Territory CoI owners on the potential use of their document identifiers in the deduplication solution.**	**Action Required**
Governance: TDIF Policies	**Issue 2: Impact on TDIF policies** The entire suite of TDIF documentation should be reviewed briefly to ensure that the impact of deduplication is addressed. Key areas will include policies on data retention, data destruction, security and audit. Galexia's view is that this issue like this highlights that the governance arrangements may need to be reviewed in order to strengthen the separation of TDIF participants, especially when TDIF participants may have multiple roles.	**Recommendation C8: The entire suite of TDIF documentation should be the subject of a brief review to assess the impact of deduplication, and updated as necessary.**	**In Progress**

[9] Note: In this PIA we have not conducted a review of state and territory data custodian rules or limitations on the use of their CoI documents.

Governance: Managing Function Creep	Privacy regulators and consumer stakeholders have consistently expressed concern about the potential for function creep in the TDIF. Deduplication is unlikely to be the main source of this concern, as there are many more damaging ways that the TDIF could be altered to become more privacy intrusive. However, any change or new use of data within the TDIF will be the subject of some caution. Deduplication does not assist any TDIF participant to track individuals across the federation, or to create new surveillance tools. One step that will help to manage function creep (and perceptions about function creep) is the introduction of a list of permitted and prohibited purposes for the deduplication data. TDIF accredited bodies would risk losing their accreditation if they used or disclosed the data in breach of these requirements (in addition to the normal Privacy Act remedies available).	Refer to Recommendation C3: Update the TDIF to include a specific section on the deduplication data – including a list of permitted uses for the data and a list of prohibited uses.	**Action Required**

C5. Deduplication: Overall Finding

Stakeholders expressed several significant concerns. We suggest this may be addressed through the recommendations – and initially through clearly documented explanations and justifications/benefits.

We have identified a number of privacy advantages to the suggested technical approach proposed by DTA:

- No additional or extra information is collected from consumers (unlike, for example, PORO Proof of Record Ownership) processes);
- The new identifier / digest that is created does not itself reveal any personal information;
- The new identifier / digest is only shared / disclosed to the Identity Exchange; and
- The Identity Exchange is not required to share / disclose the new identifier / digest.

The overall finding is that the proposed deduplication solution could proceed to the public beta – if all recommendations (including an evaluation of quality and accuracy in a pilot/trial) are implemented, without a significant privacy impact on the overall TDIF program (as it currently stands).

D. Restricted Attributes: A policy solution to establish a process for Relying Parties to seek additional and restricted attributes.

D1. Proposal Overview: To allow Relying Parties to ask for additional restricted attributes from identity providers.

DTA is proposing to allow Relying Parties to ask for additional restricted attributes from Identity Providers. Core attributes (such as name and identity proofing level) are automatically shared. Under the proposal a Relying Party could seek authority from the Oversight Authority to collect restricted attributes.

D2. Solution Overview: To require Relying Parties to show a clear business or legislative requirement for the additional restricted attribute and for these to be published in a register of authorisations.

To manage this issue DTA is proposing a number of restrictions where Relying Parties will only be granted additional restricted attributes where they can show a clear business or legislative requirement; and where the restricted attribute is approved by the Oversight Authority. The approval is limited to that specific Relying Party.

The DTA proposes to establish a public register of such authorisations.

D3. TDIF4 does not currently permit additional attributes

TDIF4 05 Role Requirements (March 2020 v1.0)

3 Identity Service Provider Requirements

3.7 Attribute disclosure

TDIF Req: IDP-03-07-01; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MAY* disclose the *Attributes* listed in the “Attributes to be collected, verified and recorded” column of Table 2 and the *Attributes* listed in Table 3 for the purpose of having them verified (i.e., with the issuer of the associated *EoI document*).

TDIF Req: IDP-03-07-01a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MUST NOT* disclose *Attributes* beyond those listed in IDP-03-07-01 for the purpose of having them verified.

TDIF Req: IDP-03-07-02; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MAY* disclose all of the following *Attributes*:

- Verified name(s).
- Verified date of birth.
- Validated contact details it collects.
- *Identity Proofing Level* achieved.
- Date and time the *Digital Identity* was created.

to a *Relying* Party via an *Identity Exchange* or *Attribute Service Provider*).

TDIF Req: IDP-03-07-03; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MAY* seek permission from the *DTA* to request the sharing of more *Attributes* than those listed in TDIF req: IDP-03-06-02.

TDIF Req: IDP-03-07-03a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MUST NOT* disclose *Attributes* beyond those listed in IDP-03-07-01 for the purpose of service delivery, unless approved by the *DTA* to do so.

D4. Additional Restricted Attributes: Findings and Recommendations Summary

Requirement	Galexia Finding	Galexia Recommendation	Status
APP 1: Open and Transparent Management of Personal Information	The APP 1 'equivalent' in the TDIF Privacy Requirements is *section 3.2.2 (Privacy Policy)* of *TDIF4 04 Functional Requirements* – although some other sections also cover broader issues of openness (such as the sections on privacy governance). *Section 3.2.2* mandates that participants publish a privacy policy containing key information. **For IdPs** The IdP privacy policies considered in this PIA already clarify that some attributes will only be shared with specific authorised RPs – not all data will be shared with all RPs. A secondary question is what the privacy policies state about consent for sharing these restricted attributes. The Australia Post Digital ID Privacy Policy[10] states: *We do not provide to the Organisation copies of ID Documents, identification numbers used on ID Documents, or details of the authentication sources used to check Your identity, unless we have Your express consent.* The myGovID Privacy Policy[11] states: *We will not share your personal information with third parties including the document issuer, the identity exchange and the online services you attempt to access, without your consent.* As can be seen, there is some inconsistency between the policies regarding the terms 'consent' and 'express consent', but the requirement, and overall message to consumers, is reasonably clear (ie. the additional restricted attributes will not be shared without consent), and the privacy policies are consistent with the requirement in section 2.9 of the TDIF Privacy Requirements regarding consent. Both Privacy Policies correctly list the type and range of attributes that might be shared (e.g., identity document numbers). **At RPs** Each RP needs to comply with APP 1, but this is unlikely to be a major challenge, and detailed consideration of this issue is outside the scope for this PIA.		**Compliant**
APP 2: Anonymity and Pseudonymity	Not applicable.		**–**

[10] Australia Post, *Digital iD™ Privacy Notice* (13 August 2020) <digitalid.com/privacy.html> and repeated in Australia Post, *Digital iD™ Terms of Use* (13 July 2019) <digitalid.com/terms/web.html>.

[11] Australian Government, *myGovID Privacy Policy* (August 2019) <www.mygovid.gov.au/mygovid-privacy-policy>.

APP 3: Collection of solicited personal information	Both APP 3 and its equivalent in section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* contain rules on the collection of personal information and data minimisation. Stakeholders have supported the development and publication of a clear set of authorisation rules. Recommendation D1 suggests three tests to be included in 'attribute authorisation' rules. In combination, these tests should have a positive impact on data minimisation. Galexia has considered a number of examples and use cases where these tests may be used to reject some specific RP tests. Overall, the data minimisation test and the suggested additional tests authorisation rules should be able to work together, and ensure that the sharing of restricted attributes is justified.	**Recommendation D1: Develop and publish clear attribute authorisation rules that incorporate data minimisation principles** RPs that require restricted attributes should justify their request and this could be included in attribute authorisation rules that incorporates data minimisation, including 3 tests: **1)** Justification of restricted attributes **2)** Demonstrate how the request for restricted attributes will meet a legislative or regulatory requirement **3)** Require that the restricted attributes will not be extended beyond those collected by IdPs in the normal course of verifying an identity	**Action Required**
APP 4: Dealing with unsolicited personal information	Not applicable.		**–**
APP 5: Notification	APP 5 sets out requirements for the notice to be given to applicants. These requirements are mirrored and slightly enhanced in section 3.5 (Notification of Collection) of the *TDIF4 04 Functional Requirements*. TDIF requires participants to meet specific notice and consent rules for attributes. In practice consumers will be presented with a notice and consent option each time a specific attribute is provided to a specific RP. There may be some options that allow consumers to provide lasting consent, and these are likely to be welcomed by consumers. The Identity Exchange will play an important role in enforcing these notice and consent rules. For example, no restricted attributes will be shared with RPs who have not met both the authorisation requirement and the consent requirement.		**Compliant**
APP 6: Use or Disclosure	APP 6 places restrictions on the use and disclosure of personal information. The TDIF Privacy Requirements place numerous additional restrictions on the use and disclosure of personal information: ● 3.6 Collection and use limitation ● 3.7 Limitation on use of behavioural information ● 3.8 Collection and disclosure of biometrics ● 3.9 Consent It is unlikely that RPs will seek restricted attributes for any uses that are prohibited by TDIF (e.g., direct marketing). Most requests for restricted attributes will be justified by reference to a specific legal requirement – this will also help to satisfy the requirements of APP 6.	**Note:** Subject to Recommendation D1: Develop attribute authorisation rules that incorporate data minimisation principles.	**Action Required**
APP 7: Direct Marketing	**Not applicable** – Section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* prohibits direct marketing		**–**
APP 8: Cross Border Disclosure	Not applicable.		**–**

APP 9: Government Related Identifiers	APP 9 places some restrictions on the use of government related identifiers by organisations. These requirements might potentially apply to some **private sector** IdPs and Relying Parties. However, APP 9 includes an important exception: *An organisation may use or disclose the government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a)).* This exception allows the organisation to ● Use a government related identifier itself (e.g., where the organisation has its own business need to verify the identity of the individual); or ● Use on behalf of a consenting User (e.g., where the organisation provides a service to assist individuals to verify their identity to third parties). Section 3.11 (Government Identifiers) of the Privacy Requirements *TDIF4 04 Functional Requirements* also include a specific restriction on government related identifiers: *An Applicant MUST NOT create a new government identifier that is used across the identity federation (i.e., an identifier that is sent to more than one Relying Party or Identity Service Provider).* The TDIF requirement is stricter than APP 9 and has been included in order to prevent the development of a national identifier (either deliberately or accidentally). In practice, some IdPs might share specific government related identifiers with specific RPs under the umbrella of sharing restricted attributes. This is because some RPs are likely to seek identity document numbers Such RPs are likely to already collect these identity document numbers from individuals, and TDIF can play a role in eliminating duplicate requests for these numbers. This type of sharing is anticipated and allowed by the exception in APP 9.2 (a). However, both APP 9 and section 3.11 of the TDIF Privacy Requirements restrict the sharing of unique government identifiers in other circumstances. Importantly, the TDIF Attribute Profile does not allow the unique identifier created by an IdP for its clients (IdP Link[12]) to be shared with RPs in the day-to-day business of the TDIF – and it is not intended for an IdP Link to be a restricted attribute and thereby accessible by RPs This is because the 'double blind' arrangements are designed to restrict RP knowledge of the IdP chosen by clients (and vice versa). Any sharing of unique IdP identifiers would obviously undermine this arrangement. However, exceptions are allowed where there is an investigation of a suspicious transaction or identity fraud. It is important that this exception is reserved for special circumstances and does not become the norm. Where an RP asks for routine access to IdP unique identifiers this request would be rejected under the authorisation rules. The authorisation rules could be clarified by including in the TDIF with an explicit reference to the alternative path for sharing attributes of this type in fraud cases. This approach would also clarify that sharing an identifier for a specific investigation is not a breach of *section 3.11* of the TDIF Privacy Requirements. Refer to H. Fraud Management.		**Further Measure Possible**
APP 10: Quality of Personal Information	APP 10 requires agencies to ensure that data is accurate and up to date in relation to the purpose for which it is collected and used. Section 3.13 (Quality of personal information) of the Privacy Requirements in *TDIF4 04 Functional Requirements* has some additional requirements for IDPs. Generally, the sharing of restricted attributes will not have a major impact on APP 10 for the TDIF. For some RP activities the sharing of key attributes (such as document expiry dates) may have a positive impact on their compliance with the APP 10 requirements for information to be 'up to date'.		**Compliant**

[12] Refer to *TDIF4 06A – Federation Onboarding Guidance* (March 2020), *Figure 6: Identity Mapping across any Identity Exchange:*

APP 11: Security	APP 11 sets a vague standard for ensuring security of personal information. The TDIF contains a range of more specific security requirements and security audit requirements, in Section 4 (Protective Security Requirements) and Section7 (Functional Assessments) of *TDIF4 04 Functional Requirements* (March 2020) and references to security considerations in other key sections of the TDIF documentation. APP 11 states that security measures should be in proportion to the risk of the information being disclosed. Overall, the inclusion of additional restricted attributes will lead to a slight rise in the risk profile of TDIF, as more data will be shared, and some of this data (if it fell into the wrong hands following a breach) might lead to increased opportunities for identity impersonation. This PIA has not considered security issues in detail. We are aware that an 'end to end' TDIF security review has been scheduled – the use of restricted attributes could be included in that review.	**Recommendation D2: Review security measures for sharing restricted attributes** Consider the proposed use of restricted attributes in the high-level security review of the digital identity environment.	**Action Required**
APP 12: Access	The proposed sharing of restricted attributes does not raise new or specific concerns regarding access and compliance with APP 12.		**Compliant**
APP 13: Correction	Not applicable.		**–**
Governance: Public register	The proposed sharing of restricted attributes may have an impact on a number of areas of privacy governance within the TDIF. **Governance Issue 1: Public register of all shared restricted attributes** Over time, the number of additional restricted attributes authorised under TDIF may become large. It will be difficult to explain all of the potential attribute pathways in a generic document, such as an IdP privacy policy. In order to increase transparency, the OA could maintain a public register of all restricted attributes that have been authorised to be shared with specific RPs, noting the relevant data fields and RPs and the date of the agreement. Stakeholders indicated that it would be preferable to additionally include a register of proposed authorisation as well as approved authorisations.	**Recommendation D3: Public register of shared restricted attributes** The OA should develop and maintain a public register of all restricted attributes that have been authorised to be shared with specific RPs. The OA should consider extending this register to include proposed authorisations.	**Action Required**
Governance: Exceptions	**Governance Issue 2: Clarifying exceptions** The TDIF has always anticipated that some restricted attributes would be shared in specific cases of identity fraud or suspicious transactions, even where these attributes are not authorised for general sharing to a RP. However, the rules for the two different types of disclosure are set out in different TDIF documents. Consumers (and potentially RPs seeking authorisation) would benefit from seeing a clear reference in the authorisation requirements to the exceptions and the alternative paths that could be followed in order to gain access to restricted attributes for a specific fraud investigation. This information could be included in the section on authorisations, with clear information on the two pathways, definitions of the two types of disclosures, and links to the relevant fraud related TDIF documents.	**Recommendation D4: Clarify exceptions to the authorisation requirements** The TDIF should clarify the circumstances in which attributes can be shared with RPs without requiring authorisation. **Note:** Subject to Recommendation D1: Develop attribute authorisation rules that incorporate data minimisation principles.	**Action Required**

Governance: Consultation	**Governance Issue 3: Consultation on authorisations** TDIF external stakeholders will expect to be consulted about the sharing of restricted attributes with RPs. Reactions may be strong – because of concerns of a gradual expansion of the TDIF (see the section on function creep below) and perceived inconsistencies with previous TDIF public statements. In practice, TDIF has always anticipated some expanded use of restricted attributes in special circumstances, but this information was relatively obscure compared to mainstream 'privacy by design' commitments. Generally, TDIF has consulted with external stakeholders through workshops and through specific consultation during TDIF PIAs. This issue will definitely need to be raised during the next round of external consultations. However, we should not rule out the need for *additional* consultation on specific requests for restricted attributes to be shared, particularly where they involve high-risk data. Some stakeholders requested a consultation on both the proposal and the authorisation process. The authorisation requirements do not include a requirement for public consultation. A generic requirement might be cumbersome and excessive, but the TDIF OA should consider engaging with external stakeholders (or requiring the RP to do so) prior to high-risk authorisations. This approach should be considered on a case-by-case basis, and additional external consultation will not be required for each request.		**Further Measures Possible**
Governance: Managing Function Creep	Privacy regulators and consumer stakeholders have consistently expressed concern about the potential for function creep in the TDIF. Managing concerns about function creep in the context of authorising the sharing of restricted attributes is going to be challenging. In many ways, each new request to share an additional attribute tends to support the stakeholder's point that function creep is inevitable. Over time, the sheer scale of additional restricted attributes may alter the overall privacy and security risk profile of TDIF. In addition, if the sharing of restricted attributes becomes widespread, the role of the 'double blind' in the TDIF may be undermined. This is because Identity Service Providers will be able to identify the Relying Parties requesting information based on the unique 'fingerprint' of the pattern of restricted attributes that have been requested. Function creep is very difficult to prevent, but some measures are available that might help to manage it: **Measure 1: Clarifying that authorisations are not precedent setting** The authorisation process could be clarified to make it clear that each individual authorisation is stand-alone, and does not set a precedent for the approval of sharing the same attributes at a different RP. **Measure 2: Prohibiting retrospective authorisations** The authorisation requirements could include a prohibition on sharing restricted attributes retrospectively. The process should always require individual consent. In practice the TDIF lends itself to this form of consent management but enshrining it in the rules will provide another layer of confidence. **Measure 3: Encouraging reviews of authorisations every three years** Relying Parties should be encouraged by the Oversight Authority to review their continued need for restricted attributes. This will guard against complacency and drift and may allow the sharing of some attributes to be dropped where they are no longer relevant or where the risk profile has changed. The review should occur every three years, but decisions to drop restricted attributes that have been authorised should remain with the RP. **Measure 4: Imposing strict data retention requirements** The authorisation should include the ability to impose strict data retention periods. This issue is the subject of ongoing discussion in TDIF (and in the main PIAs) and it is flagged here as a potential measure to protect against function creep. In practice, TDIF does not accredit RPs, so imposing data retention periods on attributes will be challenging, but it could be achieved as an authorisation requirement.	**Recommendation D5: Expand authorisation requirements to manage function creep** Expand the authorisation requirements for sharing restricted attributes to include additional precautions against function creep. This should include: **1)** Clarifying that authorisations are not precedent setting **2)** Prohibiting retrospective authorisations **3)** Encouraging a review of authorisations every three years **4)** Imposing strict data retention requirements **5)** Limiting justifications to specific RP legislation and business needs **6)** Clarifying excluded attributes **Note:** Subject to Recommendation D1: Develop attribute authorisation rules that incorporate data minimisation principles.	**Action Required**

	Measure 5: Limiting justifications to specific RP legislation and business needs Recommendation D1 authorisation requirements suggest a requirement for RPs to justify their requests by pointing to a legislative and business need. To manage function creep, it may be necessary to clarify that this requires reference to specific RP legislation and business needs, rather than generic needs. It is Galexia's view that these types of generic requirements should not be accepted as justification and that identification of specific RP legislation should be the preferred approach. Additionally, Galexia considers it is important that the sharing of restricted attributes proceeds on a per Agency basis, rather than a Whole of Government basis. If the sharing of a specific attribute can be justified using generic legislation for one Agency, then there is a real risk that other Agencies may seek the same attribute. In order to protect privacy and send a clear message to Relying Parties about data minimisation, they should be required to point to specific Agency legislation or business requirements. **Measure 6: Clarifying excluded attributes** It may also be useful to include a set of excluded attributes where authorisation will not be granted – such as device information, IP addresses and IdP client identifiers (this information may be sought using the alternative fraud investigation pathway). Having a visible list of prohibited items can often help in managing function creep and improving privacy perception issues.		

D5. Restricted Attributes: Overall Finding

Overall, this PIA has found that the proposed approach to managing the sharing of restricted attributes should be subject to the establishment of attribute authorisation rules/framework.

It will be challenging to communicate the authorisation process to external stakeholders – who have strong concerns about function creep in the overall TDIF program. Although the TDIF has always envisaged the need to share some restricted attributes with specific Relying Parties in special circumstances, this policy has not been directly communicated to external stakeholders.

There will be strong opposition to the authorisation of sharing key attributes such as document identifiers, even in circumstances where RPs already collect these attributes. This PIA includes some recommendations to help manage these concerns, but they are unlikely to completely remove stakeholder concerns and potential opposition.

Also, authorising the sharing of restricted attributes does raise the overall security and privacy risk profile of TDIF, and care is needed to ensure specific RP requests do not undermine the privacy enhancing and privacy by design elements of the overall Framework.

If the package of recommendations is implemented, Galexia has identified several privacy advantages to this proposed approach taken to managing the sharing of restricted attributes in the TDIF:

- Specific authorisation would be required for each additional attribute at each Relying Party (RP) – there is no allowance for the generic approval of restricted attributes across multiple RPs;
- All restricted attributes can only be shared with consent – with some appropriate exceptions related to the investigation of identity fraud;
- The onus is on RPs to justify the need for restricted attributes and to demonstrate that they are managing privacy, legal and risk issues;
- The RPs cannot seek any restricted attributes that are not already collected by Identity Service Providers (IdPs) in the normal course of verifying an individual's identity; and
- Some core TDIF privacy principles are maintained (e.g., data minimisation requirements and restrictions on the use of identifiers across the federation).

Additionally, refer to H. Fraud Management.

E. Biometrics: Proposal to manage the use and retention of biometric data presented during proofing.

E1. Proposal Overview: To allow Identity Providers to check presented photos against photos held in a document chip or against images held in the Face Verification Service.

DTA has confirmed and expanded the requirement for biometric proofing when a User first registers for a digital identity. Refer below to E3. *TDIF4 05 Role Requirements (March 2020 v1.0)*, Appendix B: Biometric verification requirements.

The requirements now include:

1) Identity Providers must employ presentation attack detection technology to determine if the presented photo (known as the Acquired Image) is of a living human subject present at the point of capture.

2) Identity Providers must use a biometric matching algorithm to perform one-to-one verification matching between the Acquired Image and the Photo ID image.

3) Identity Providers can check the Acquired Image against either a photo stored in an RFID chip (e.g., for Passports) or an image held in an appropriate document via the Face Verification Service (FVS).

E2. Solution Overview: To prohibit one-to-many matches and impose other strict requirements on Identity Providers.

To manage this issue DTA is imposing the following requirements:

1) Identity Providers must NOT use a biometric matching algorithm to perform one-to-many matching against a database of reference images as part of the biometric binding process.

2) Identity Providers must achieve a false match rate of not more than 0.01% and a false non-match rate of not more than 3%.

3) Identity Providers must NOT retain any Personally Identifiable Information captured in biometric binding processes.

4) Identity Providers are responsible for the destruction of all Biometric Samples, including any subcontractors or third-party components.

E3. *TDIF4 05 Role Requirements (March 2020 v1.0),* Appendix B: Biometric verification requirements

<www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework/framework-documents>

This Appendix sets out requirements to confirm the link between the *Individual* and the *Identity* being claimed using *Biometric verification.*

B1. Requirements for biometric binding

B1.1 Requirements for online biometric binding

***TDIF* Req:** IDP-03-09-01; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* restrict access to the control of any aspects of the Biometric Capability exclusively to *Assessing Officers* that have completed the appropriate training pertaining to the exercise of such control.

***TDIF* Req:** IDP-03-09-02; **Updated**: Mar-2020; **Applicability**: I
To complete *Online Biometric binding* the *Applicant MUST* either:

- capture and send the *Acquired image* to the Photo ID Authoritative Source (or proxy) in the case of *source biometric matching*; or,
- capture and perform *document biometric matching* of the *Acquired Image* against the image read directly from the Photo ID RFID chip.

***TDIF* Req:** IDP-03-09-03; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* incorporate *presentation attack detection* when performing *Online Biometric binding.*

***TDIF* Req:** IDP-03-09-04; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* complete the image capture and *presentation attack detection* processes as part of the same process before submission to *Online Biometric binding*. This is to prevent attacks that would exploit the separation of the *presentation attack detection* and the image acquisition.

B1.2 Requirements for presentation attack detection

***TDIF* Req:** IDP-03-09-05; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* employ *presentation attack* detection technology to determine if the *Acquired image* is of a living human subject present at the point of capture.

***TDIF* Req:** IDP-03-09-06; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* include liveness detection processes as part of *presentation attack* detection.

***TDIF* Req:** IDP-03-09-07; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* employ *presentation attack* detection technology that includes data capture and system level monitoring as described by ISO 30107-1.

***TDIF* Req:** IDP-03-09-08; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* ensure that the presentation attack detection technology meets the requirements of at least Evaluation Assurance Level 1 as described by ISO 30107-3.

***TDIF* Req:** IDP-03-09-08a; **Updated**: Mar-2020; **Applicability**: I
If the comprehensive risk assessment undertaken by the *Applicant* indicates that the *presentation attack detection* technology used in the capability must exceed these standards, the *Applicant* *MUST* meet the requirements described in the risk assessment.

***TDIF* Req:** IDP-03-09-09; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* capability *MUST* have been tested by a qualified third-party testing entity with experience in biometric testing and ISO 30107 to determine that the *presentation attack detection* technology meets the requirements for at least Evaluation Assurance Level 1 of ISO 30107-3.

***TDIF* Req:** IDP-03-09-09a; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* have determined *presentation attack detection* outcomes in a trusted computing environment.

***TDIF* Req:** IDP-03-09-09b; **Updated**: Mar-2020; **Applicability**: I
All testing performed *MUST* have been performed on a solution that incorporates all hardware and software involved in the *biometric binding* process including the *presentation attack detection* technology and *biometric matching*.

***TDIF* Req:** IDP-03-09-09c; **Updated**: Mar-2020; **Applicability**: I
Any determinations made by manual processes *MUST* be recorded separately to the *biometric matching* or *presentation attack detection* systems.

***TDIF* Req:** IDP-03-09-10; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* provide a report to the *DTA* as part of initial accreditation from the qualified third-party testing entity outlining that the *Applicant*'s *presentation attack detection* technology has been suitably tested to the specifications of at least Evaluation Assurance Level 1 of ISO 30107-3.

***TDIF* Req:** IDP-03-09-10a; **Updated**: Mar-2020; **Applicability**: I
The report *MUST* describe the completed *presentation attack detection* evaluation and corresponding results for each presentation attack type with the closest possible adherence to reporting specifications as described in ISO 30107-3.

***TDIF* Req:** IDP-03-09-10b; **Updated**: Mar-2020; **Applicability**: I
The report *MUST* be completed annually thereafter and provided to the *DTA* as part of the *Annual Assessment*.

B1.3 Requirements for document biometric matching

***TDIF* Req:** IDP-03-09-11; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* verify the authenticity of the image read from the Photo ID RFID chip according to the Photo ID Issuing Authority instructions.

***TDIF* Req:** IDP-03-09-12; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* only process Claimed Photo ID through *document biometric matching* that contain a government issued and cryptographically signed image, such as an ePassport.

***TDIF* Req:** IDP-03-09-13; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* use a *biometric matching* algorithm to perform one-to-one verification matching between the *Acquired image* and the Photo ID image.

***TDIF* Req:** IDP-03-09-14; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST NOT* use a *biometric matching* algorithm to perform one-to-many matching against a database of reference images as part of the *biometric binding* process.

***TDIF* Req:** IDP-03-09-15; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* ensure their *biometric matching* algorithm is tested by a qualified third-party testing entity to determine the failure to enroll rate (if applicable), failure to acquire rate, false match rate and false non-match rate of the capability as per the reporting specification described in ISO 19795.

***TDIF* Req:** IDP-03-09-15a; **Updated**: Mar-2020; **Applicability**: I
This *MUST* be tested under production-like conditions.

***TDIF* Req:** IDP-03-09-15b; **Updated**: Mar-2020; **Applicability**: I
The minimum number of subjects for the testing *MUST* be 245, as described in FIDO Biometric Requirements.

***TDIF* Req:** IDP-03-09-15c; **Updated**: Mar-2020; **Applicability**: I
The testing *MUST* be performed in a verification scenario with comparable image types to production expectations.

***TDIF* Req:** IDP-03-09-16; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* achieve a false match rate equivalent to or lower than FIDO Biometric Requirements. This requires a false match rate of not more than 0.01% and a false non-match rate of not more than 3%.

***TDIF* Req:** IDP-03-09-016a; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* record *biometric matching* outcomes in a trusted computing environment.

B.2 Photo ID specific requirements

***TDIF* Req:** IDP-03-09-17; **Updated**: Mar-2020; **Applicability**: I
Where the Photo ID used has an RFID chip that is available and functional, the *Applicant MUST* perform a biometric match of the *Acquired image* only against the image read directly from the Photo ID RFID chip.

***TDIF* Req:** ID-03-09-17a; **Updated**: Mar-2020; **Applicability**: I
Where an RFID chip is not available, the Photo ID image used for *biometric matching MUST NOT* be from a scan of a physical document.

***TDIF* Req:** IDP-03-09-18; **Updated**: Mar-2020; **Applicability**: I
Where the Photo ID used is an Australian ePassport, the *Applicant MUST* check the Country Signing Certification Authority (CSCA) Certificate as per ICAO document validation guidelines OR perform a DVS check. Where the Australian ePassport security certificate is checked, the Australian Certificate Revocation List must also be checked.

***TDIF* Req:** IDP-03-09-18a; **Updated**: Mar-2020; **Applicability**: I
Where an RFID chip is not available, non-functional or the document security is lower than that of the Australian ePassport, a DVS check *MUST* be performed by the *Applicant*.

***TDIF* Req:** IDP-03-09-18b; **Updated**: Mar-2020; **Applicability**: I
A DVS check *MUST* be performed by the *Applicant* where the Photo ID used is a foreign ePassport to ensure that the foreign ePassport is linked to a current visa.

***TDIF* Req:** IDP-03-09-18c; **Updated**: Mar-2020; **Applicability**: I
Where the Photo ID used is a foreign ePassport and an RFID chip is not available or non-functional the *Applicant* *MUST* attempt to perform a biometric match against the corresponding image recorded against that identity from the Photo ID Authoritative Source.

***TDIF* Req:** IDP-03-09-18d; **Updated**: Mar-2020; **Applicability**: I
Where the Photo ID used is a foreign ePassport and an RFID chip is not available or non-functional and the corresponding image recorded against that identity from the Photo ID Authoritative Source is unavailable, the *Applicant* *MUST* perform Local *Biometric binding*.

B3 Image quality specific requirements

***TDIF* Req:** IDP-03-09-19; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* produce an *Acquired image* quality profile informed by the properties and characteristics described by ISO 29794-5 which details a set of minimum standards that the *Acquired image* must meet before *biometric matching*.

***TDIF* Req:** IDP-03-09-20; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* include automated quality controls and appropriate user-interface instructions that directs Users to provide an image that meets the *Acquired image* quality profile.

B3.1 Requirements for Local Biometric Binding

***TDIF* Req:** IDP-03-09-21; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* perform source *biometric matching* to supplement Manual Face Comparison by performing a biometric match against the corresponding image recorded against that identity from the Photo ID Authoritative Source.

***TDIF* Req:** IDP-03-09-22; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* perform a DVS check as part of the Local *Biometric binding* process to confirm the authenticity of a Photo ID.

***TDIF* Req:** IDP-03-09-23; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* train relevant Assessing Officer's on Manual Face Comparison techniques including, but not limited to:

- Techniques for *Individual* feature comparison
- Awareness of racial and cognitive biases
- Presentation attack indicators
- Guided matching examples

The training material *MUST* be provided by the *Applicant* to the *DTA* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

B4 Requirements for logging and data retention

***TDIF* Req:** IDP-03-09-24; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* maintain the information associated with each *Individual* transaction, including a log of activities that details which Assessing Officer collected data, what data was collected, when and where the data was collected.

***TDIF* Req:** IDP-03-09-24a; **Updated**: Mar-2020; **Applicability**: I
This log *MUST NOT* include Biometric Samples.

***TDIF* Req:** IDP-03-09-25; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* have in place audit or random checking procedures to help detect fraud or inadequate Manual Face Comparison and verification by *Assessing Officers*.

***TDIF* Req:** IDP-03-09-26; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST NOT* retain any Personally Identifiable Information captured in *biometric binding* processes.

***TDIF* Req:** IDP-03-09-27; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* ensure that it is responsible for the destruction of all Biometric Samples, including all copies, caches, and intermediary databases, including any subcontractors or third-party components.

***TDIF* Req:** IDP-03-09-27a; **Updated**: Mar-2020; **Applicability**: I
This destruction process *MUST* be documented by a specific audit log.

***TDIF* Req:** IDP-03-09-27b; **Updated**: Mar-2020; **Applicability**: I
The *Acquired image MUST*, unless required by law, then be destroyed consistent with *TDIF* Req: PRIV-03-08-02.

B5 Manual Face Comparison specific requirements

***TDIF* Req:** IDP-03-09-28; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MAY* utilise manual processors performed by *Assessing Officers* to complete Local *Biometric binding* or Online *Biometric binding* processes.

***TDIF* Req:** IDP-03-09-29; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MAY* utilize manual processors to review and/or adjust decisions made by the *Applicant* Capability, including biometric match results and *presentation attack detection*.

***TDIF* Req:** IDP-03-09-30; **Updated**: Mar-2020; **Applicability**: I
The *Acquired image MUST NOT* be retained after completion of the *Local Biometric Binding* or Online *Biometric binding* processes by the Assessing Officer.

***TDIF* Req:** IDP-03-09-31; **Updated**: Mar-2020; **Applicability**: I
If the *Applicant* utilises any manual processes, The *Applicant MUST* include this in their risk assessment for *biometric binding* processes.

***TDIF* Req:** IDP-03-09-32; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* maintain an audit log of manual processes that meets the requirements of the *TDIF*. This includes records of transactions in production and the training activities of *Assessing Officers*. The audit log *MUST* be auditable by the *DTA*.

***TDIF* Req:** IDP-03-09-33; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* only perform remote Manual Face Comparison for Online *Biometric binding* after attempting a Biometric Match.

***TDIF* Req:** IDP-03-09-34; **Updated**: Mar-2020; **Applicability**: I
The *Applicant MUST* only undertake remote Manual Face Comparison utilizing *Assessing Officers* located within Australia.

E4. Biometrics and Proofing: Findings and Recommendations Summary

Requirement	Galexia Finding	Galexia Recommendation	Status
Categorisation of Data	Complying with the Privacy Act and TDIF Functional Requirements on privacy requires participants to identify the data they collect and categorise the data – usually into personal information, sensitive personal information (in TDIF this category usually only applies to biometric data) and non-personal information. For example, section 3.2.1 (Privacy Governance) of *TDIF4 04 Functional Requirements* requires participants to *maintain a record of personal information holdings* Some of the data collected in the Digital Identity ecosystem is biometric information and this is categorised as 'sensitive' information for the purposes of the Privacy Act.		

	The categorisation of data as sensitive data has impacts under APP 3, APP 6 and APP 9, and these are discussed in more detail in the relevant sections below.		
APP 1: Open and Transparent Management of Personal Information	The APP 1 ‘equivalent’ in the TDIF Privacy Requirements is section 3.2.2 (Privacy Policy) of *TDIF4 04 Functional Requirements* – although some other sections also cover broader issues of openness (such as the sections on privacy governance). *Section 3.2.2* mandates that participants publish a privacy policy containing key information. The collection, use, disclosure and destruction of biometric information must be described in the relevant Identity Provider privacy policy. This aspect of the Digital Identity ecosystem has been in place for some time, and privacy policies have been prepared with the use of biometrics in mind. The approach does not include significant changes regarding the collection of biometric information, apart from the ability to conduct a one-to-one match between the presented photo and a photo contained in the RFID chip of an identity document (e.g., a passport). This minor change does not necessitate a rewrite of privacy policies, as it is likely to be covered by the Privacy Notice and other information presented at the time of registration. However, privacy policies should be reviewed for accuracy in case any specific information or promises have been included in existing policies that might now be inaccurate (for example, privacy policies may have promised that images would only be matched via the Face Verification Service (FVS).	**Recommendation E1: Identity Provider privacy policies should be reviewed to ensure that promises made about biometric image matching remain accurate.** This is required as Identity Providers are permitted to use one-to-one matching between the presented image and an image stored in the RFID chip of an identity document.	**Action Required**
APP 2: Anonymity and Pseudonymity	Not applicable – The TDIF is an identity framework designed to cater for transactions that require Level 2 and Level 3 identity. There is no expectation that anonymity or pseudonymity will be made available to consumers in transactions at this level.		**–**
APP 3: Collection of solicited personal information	Both APP 3 and its equivalent in section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* contain rules on the collection of personal information and data minimisation. Section 3.8 (Collection and disclosure of biometrics) of *TDIF4 04 Functional Requirement*s contains a requirement of **explicit** consent: *The Applicant [Identity Exchange] MUST only collect Sensitive information (including Biometric information) as outlined in APP 3.3 and 3.4.* As a result, the requirement for allowing individuals to opt-in to enduring consent will need to require the explicit consent of the individual. It cannot be implied or inferred consent. Accredited Identity Providers already have explicit consent processes in place for biometric image collection and this proposal should not have a significant impact on the collection of explicit consent. APP 3 also includes a data minimisation requirement. This requirement is strengthened by the TDIF requirements to impose strict limits on the collection of biometric information so that only one to one matching can be performed: ***TDIF* Req:** IDP-03-09-14; **Updated**: Mar-2020; **Applicability**: I The *Applicant MUST NOT* use a *biometric matching* algorithm to perform one-to-many matching against a database of reference images as part of the *biometric binding* process.		**Compliant**
APP 4: Dealing with unsolicited personal information	Not applicable		–
APP 5: Notification	APP 5 sets out requirements for the notice to be given to applicants. These requirements are mirrored and slightly enhanced in section 3.5 (Notification of Collection) of the *TDIF4 04 Functional Requirements*. The current privacy notices disclose arrangements for the collection, storage and destruction of biometric information. However, they will need to be reviewed and updated to reflect the use of images contained in RFID chips of Identity documents. Previously the TDIF only used image matching via the Face Verification Service (FVS).	**Recommendation E2: Review and update Identity Provider privacy notices to reflect the potential use of images contained in RFID chips of Identity documents.**	**Action Required**

APP 6: Use or Disclosure	APP 6 places restrictions on the use and disclosure of personal information. The Privacy Requirements in *TDIF4 04 Functional Requirements* place numerous additional restrictions on the use and disclosure of personal information: ● 3.6 Collection and use limitation ● 3.7 Limitation on use of behavioural information ● 3.8 Collection and disclosure of biometrics ● 3.9 Consent There are no significant changes relevant to APP 6 resulting from the proposed use of images contained in RFID chips of Identity documents.		**Compliant**
APP 7: Direct Marketing	**Not applicable** – Section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* prohibits direct marketing.		**–**
APP 8: Cross Border Disclosure	**Not applicable** – This proposal does not raise any specific issues relevant to APP 8.		**–**
APP 9: Government Related Identifiers	**Not applicable** – This proposal does not raise any specific issues relevant to APP 9.		**–**
APP 10: Quality of Personal Information	APP 10 requires agencies to ensure that data is accurate and up to date in relation to the purpose for which it is collected and used. While section 3.13 (Quality of personal information) of the Privacy Requirements in *TDIF4 04 Functional Requirements* has some additional requirements for IDPs, these do not all apply to the Exchange. The TDIF4 Biometric verification requirements permits some very limited additional biometric matching (e.g., between the presented image and an image stored on a document's RFID chip). However, this greater flexibility is accompanied additional requirements, including rules on data quality: ***TDIF* Req:** IDP-03-09-16; **Updated**: Mar-2020; **Applicability**: I The *Applicant MUST* achieve a false match rate equivalent to or lower than FIDO Biometric Requirements. This requires a false match rate of not more than 0.01% and a false non-match rate of not more than 3%.		**Compliant**
APP 11: Security	APP 11 sets a somewhat vague standard for ensuring security of personal information. The TDIF contains a range of more specific security requirements and security audit requirements, in Section 4 (Protective Security Requirements) and Section7 (Functional Assessments) of *TDIF4 04 Functional Requirements (March 2020)* and references to security considerations in other key sections of the TDIF documentation. APP 11 states that security measures should be in proportion to the risk of the information being disclosed. The security arrangements for the collection, storage and destruction of biometric information will need to be reviewed and updated to reflect the use of images contained in RFID chips of Identity documents. Previously the TDIF only used image matching via the Face Verification Service (FVS) – which only provides a yes / no answer to a match and therefore provides a high degree of security and privacy. The use of images held on RFID chips might raise new security issues or vulnerabilities, as the person presenting the document may be engaged in an attempt to acquire a fraudulent digital identity by presenting fake or altered identity documents. Removing the FVS check would appear to remove an opportunity for some types of fraud to be detected. APP 11 and TDIF Biometric verification requirements also impose data retention and destruction requirements for biometric information: ***TDIF* Req:** IDP-03-09-26; **Updated**: Mar-2020; **Applicability**: I The *Applicant MUST NOT* retain any Personally Identifiable Information captured in *biometric binding* processes. ***TDIF* Req:** IDP-03-09-27; **Updated**: Mar-2020; **Applicability**: I The *Applicant MUST* ensure that it is responsible for the destruction of all Biometric Samples, including all copies, caches, and intermediary databases, including any subcontractors or third-party components.	**Recommendation E3: The security arrangements for the collection, storage and destruction of biometric information should be reviewed and updated to reflect the proposed use of images contained in RFID chips of Identity documents.**	**Action Required**

APP 12: Access	Section 3.12.1 (Access) in *TDIF4 04 Functional Requirements* addresses some of the limitations in APP 12, requiring all participants to meet higher access standards and enabling a more consistent experience for users. The (minor) changes to the collection, use and destruction of biometric information should have no impact on access rights under APP 12.		**Compliant**
APP 13: Correction	Sections 3.12.2 (Correction) and 3.14 (Handling Privacy Complaints) in *TDIF4 04 Functional Requirements* (March 2020) contains additional requirements to APP 13, establishing a higher standard of corrections and complaints that TDIF participants must comply with. The (minor) changes to the collection, use and destruction of biometric information should have no impact on correction rights under APP 13.		**Compliant**

E5. Biometrics and Proofing: Overall Findings

Galexia’s view is that the change to the collection, use and destruction of biometric images is relatively minor.

Previously the only image matching that could be undertaken was a one-to-one match between the presented image and the original image store (e.g., a repository of driver licence images) via the face verification Service (FVS).

Under the TDIF4 Biometric verification requirements, Identity Providers are able to conduct an alternative one-to-one match between the presented image and an image stored in a reliable Identity document (e.g., an image stored in the RFID chip of a passport). This has limited privacy impact, although it will require an additional security review to be conducted to check for any new vulnerabilities.

Stakeholder concerns should be addressed by the prohibition on one-to-many matching and tougher rules on data quality and the immediate destruction of biometric images. Some stakeholders remain opposed to the use of biometrics in the TDIF. Other stakeholders queried the scope and type of biometrics that could be used – and this sends an important message to DTA about ongoing community and stakeholder education – currently the *TDIF4 05 Role Requirements – B1.3 Requirements for document biometric matching* limit biometric binding to a Photo ID.

The overall package of TDIF4 Biometric verification requirements should have a positive privacy impact, with:

- A restriction of all matching to one-to-one matches; and
- Two privacy positive measures related to data quality and data destruction

F. Governance Oversight: A staged approach to the management of key privacy issues via governance and oversight mechanisms.

F1. Proposal Overview: To manage governance arrangements in two stages, starting with the establishment of an Interim Oversight Authority.

DTA is proposing to manage governance arrangements in two stages

- **Stage 1: An Interim Oversight Authority (IOA) in place under a Program Governance** – Memorandum of Understanding between DTA and Services Australia. This Interim stage only supports the use of the system by Commonwealth government agencies and limited testing / pilots with non-Commonwealth entities.
- **Stage 2: Establishment of a permanent Oversight Authority (OA)** – potentially under a legislative framework to support model transition to the future state, delivering a more integrated, mature state in readiness for non-Commonwealth participants joining the Digital Identity system. [Note: Any potential legislative framework would be the subject of additional stakeholder consultation and is not the focus of this PIA.]

F2. Solution Overview: To give key powers to the Interim Oversight Authority.

To manage this issue DTA is proposing that privacy oversight is included within the interim Program Governance arrangements in accordance with the division of responsibilities between the DTA and Services Australia in their roles as the Interim Oversight Authority (IOA). DTA will retain accountability for the Digital Identity system. In practice this means that where a privacy issue is a policy, platform or accreditation issue it will be overseen by DTA. Where it is a direct User experience issue or is related to fraud or cybersecurity it will be overseen by Services Australia.

DTA will retain accountability for the Digital Identity system and be responsible for: ● Policy and strategy; ● Platform architecture; and ● Accreditation & termination of participants.	Services Australia will play an important role and be responsible for managing: ● ICT Service Delivery and user support; ● Fraud management; ● Cyber security; and ● Complaints by end Users

F3. Governance Oversight: Findings and Recommendations Summary

In PIA1 (2016), recommendations were made about Governance Arrangements (Recommendation 23) and this included addressing the following:

A. *Ensuring complete structural separation between the Identity Exchange and IdPs;*

B. *Ensuring an independent process is in place for TDIF accreditation;*

C. *Developing an appropriate underlying legal authority for the TDIF;*

D. *Developing appropriate coordination mechanisms for access and correction requests amongst TDIF participants, including the ability to share complaints data; and*

E. *Developing an appropriate mechanism for TDIF membership and ongoing engagement with stakeholders.*

In PIA2 (2018) both an Interim Operating Authority (IOA) and Operating Authority (OA) was briefly discussed:

> *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).***

Several recommendations relevant to Governance were made in PIA2:

> ***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.*

The PIA identified specific privacy protections to be enshrined in legislation:

> ***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; and*
>
> ***5)*** *The restrictions on the use of identifiers.*

PIA2 made a number of additional recommendations relevant to Governance

> ***Recommendation 30:*** ***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.*
>
> ***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.*

We note that the following was contained in Section 2.1 (General Requirements) of TDIF3:

> *Identity Exchanges MUST operate separately from other identity federation participants and MUST establish and maintain its own privacy management arrangements.*

Galexia could not identify an equivalent requirement in TDIF4. This potentially reduces the stricter separation requirements from TDIF3 and clear recommendations from PIAs 1 & 2. We recognise that Section 3.2.2 (Privacy Policy) in TDIF4 does have a separation requirement with respect to privacy policies – but not to the extent of separate privacy management arrangements and operational separation requirements contained in earlier releases of the TDIF.

While progress has been made with respect to progressing a Digital Identity legislative framework, Galexia is drawing attention to the earlier recommendations and to persistent stakeholder concerns around governance, particularly around the following items:

- Strengthening of separation arrangements – this goes to separation between participants (particular the exchange) an independent Oversight Authority and even the functions of the Oversight Authority. There is some variance in the strength of opinion held about the level of independence.
- Role of the Privacy Commissioner (and possible State privacy regulators)

There is particularly strong criticism about the establishment of a ‘temporary interim oversight authority’. Stakeholders considered the establishment and nature of the IOA was not well communicated. There are distinct concerns about Services Australia fulfilling the role of IOA.

We note that there have been developments with the proposed governance model in the proposed Digital Identity legislation and stress the importance of considering stakeholder views.

The underlying concern is a perception of lack of independence in any ‘oversight authority’ with responsibilities to hold a separate branch or division of itself accountable.

Common stakeholder themes about a permanent Oversight Authority include:

- Establishing the OA from the start, rather than commencing with the IOA – with a concern that a ‘stronger’ version of an oversight authority will not be introduced and the IOA may end up being the default;
- Concern that features are being added ‘out-of-sight’ under and IOA which are then impossible to remove when the replacement OA is introduced;
- Establishing separation and independence;
- Clear accountability and transparency;
- Possessing adequate powers of compliance monitoring, enforcement and disqualification;
- The OA needs to be adequately resourced; and
- Clarifying the role of the OAIC

Many of these issues are being addressed / progressed through DTA consultation on the broader legislative and governance arrangements. DTA will need to maintain close consultation with stakeholders as the governance arrangements are finalised.

G. Fraud Management: A policy and technical proposal to enhance the fraud management function in Stage 1 of the Digital Identity system.

The Interim Oversight Authority is exploring proposals to enhance and utilise the system in fraud management arising from relying party use of the system.

G1. Proposal Overview: To enhance the fraud management function in Stage 1 of the Digital Identity system, to be overseen by the Oversight Authority.

The Interim Oversight Authority is proposing to enhance the Fraud Management function in Stage 1 of the Digital Identity system (Stage 1 is the period when participation is limited to Commonwealth Agencies). The function is currently being run by the Interim Oversight Authority, who has the responsibility for conducting investigations into identity fraud and suspicious transactions.

The function will allow the 'double blind' to be lifted in some circumstances so that information can be shared with relevant participants either during or following a fraud investigation.

G2. Solution Overview: To include a clear definition of fraud, restrict the use of personal information and only lift the 'double blind' in three limited circumstances.

To manage this issue the Interim Oversight Authority is proposing that the Fraud Management function in Stage 1 of the Digital Identity system will be subject to the following controls:

1) There will be an agreed and transparent definition of fraud;

2) Personal information will only be used for investigations, not for proactive monitoring or surveillance;

3) The double blind will only be lifted in three limited circumstances

   i) To investigate a suspicious transaction;

   ii) To inform relevant parties about the result of an investigation; or

   iii) To manage a system wide attack (e.g., a major cyber security incident).

G3. Fraud Management: Findings and Recommendations Summary

Requirement	Galexia Finding	Galexia Recommendation	Status
Categorisation of Data	Complying with the Privacy Act and TDIF Functional Requirements on privacy requires participants to identify the data they collect and categorise the data – usually into personal information, sensitive personal information (in TDIF this category usually only applies to biometric data) and non-personal information. For example, section 3.2.1 (Privacy Governance) of *TDIF4 04 Functional Requirements* requires participants to *maintain a record of personal information holdings* The categorisation of data has impacts under APP 3, APP 6 and APP 9. The OA will develop and maintain a secure portal for managing information requests from Users, TDIF participants and third parties related to fraud – and this is covered in the System and Program Governance MOUs. This process will benefit from a process that categorises data to ensure that personal data and sensitive data are treated appropriately. This process is in development. **Note:** The exact data fields that may be collected, logged, used and disclosed in the proposed fraud management solution for the digital identity system are being considered. They should be the subject of further consideration on the privacy impacts in an additional PIA on the fraud management solution. Refer to Recommendation G8.		**In progress**

APP 1: Open and Transparent Management of Personal Information	APP 1 and the equivalent section of the TDIF Privacy Requirements mandate that participants publish a privacy policy containing key information. TDIF PIA1 stated: ***Recommendation 11: Secondary use for investigating identity fraud and suspicious transactions*** *The exact scope and rules for the investigation of identity fraud and suspicious transactions by TDIF participants should be addressed in the TDIF Core Service Requirements and other TDIF documentation.* ***The extent of this secondary use should be disclosed to consumers.*** The digital identity system is in the early stages of roll out, so the current privacy policies for participants are limited. For example, as of September 2020 there is no public facing privacy policy for the Exchange. Two IdPs have been accredited – Australia Post Digital iD and the ATO's myGovID. The Australia Post Digital iD is subject to a Privacy Notice,[13] rather than a privacy policy (there is also a generic Australia Post privacy policy). It does not contain any general information on fraud or suspicious transactions – however it does contain a brief mention of law enforcement access: *You hereby authorise us to disclose the information we hold about You and grant access to Your Profile to law enforcement and government authorities and agencies in accordance with their lawful requests.* The myGovID Privacy Policy[14] includes a more detailed coverage of fraud management. It states: *We collect your personal information to … investigate and verify the operation of the myGovID system.* *…* *We may use this information to … identify and respond to issues that may indicate authentication integrity is at risk; and detect, investigate, and prosecute criminal offences.* *We may share this information with GovPass MOU Participants*. To comply with APP 1, TDIF Participants will need to include information in privacy policies on the data fields that might be collected and made available (and to whom) for fraud management. The ATO's myGovID approach is a suitable template, although more detail may be required on the exact data fields (once they are determined).	**Recommendation G1: Key TDIF Participants (IdPs and the Exchange) should update privacy policies to be open about the use of some digital identity system data for fraud management.** The privacy policies should disclose (or link to) the data fields that might be shared for fraud management and the data retention periods that apply to this activity.	**Action Required**

[13] Australia Post, *Digital iD™ Privacy Notice* (13 August 2020) <digitalid.com/privacy.html> and repeated in Australia Post, *Digital iD™ Terms of Use* (13 July 2019) <digitalid.com/terms/web.html>.

[14] Australian Government, *myGovID Privacy Policy* (August 2019) <www.mygovid.gov.au/mygovid-privacy-policy>.

APP 1: Open and Transparent Management of Personal Information	A secondary issue is that consumers would benefit from consumer-friendly information on the overall digital identity system approach to fraud management, including information and links on how to report a suspicious transaction. *The TDIF4 04 Functional Requirements* set out some basic requirements for participants in relation to fraud management: ***2.4 Fraud monitoring and detection*** *The Applicant MUST implement a mechanism for detecting incidents of fraud or suspected fraud, including a process for Personnel and users to report suspected fraud confidentially.* ***2.6 Support for victims of identity fraud*** *a) The Applicant MUST implement a process which allows Users to notify it when they suspect or become aware of fraudulent use of their Attributes, Digital Identity or Credentials.* *b) The Applicant MUST provide (either directly or through a third party) support services to Users whose Attributes, Digital Identity or Credential have been compromised.* c) *The Applicant MUST have in place processes such as appropriate identification of an Individual whose Attributes, Digital Identity or Credential has been compromised and appropriate technologies to enable the applicant to flag the Attributes, Digital Identity or Credential as compromised.* d) *The Applicant MUST prevent the fraudulent use of a User's Attributes, Digital Identity or Credentials (including continued fraudulent activity) once the Applicant suspects or it becomes aware of the fraudulent use.* *e) When an Individual is identified by the Applicant as a victim of fraud, or the Individual self- identifies, their existing record MUST be reproofed to the highest Identity Proofing Level which they have previously met.* In practice the individual IdPs have chosen to include some limited information on fraud in their terms and conditions. This could be complemented by a more centralised source of information for consumers. The Australia Post Digital iD Terms and Conditions[15] state: ***7. Security*** *…* *7.6 You must notify us immediately by sending an email to help@digitalid.com if:* *a)* ***…*** b) *You suspect or have reason to believe there has been or might be any unauthorised or fraudulent use of Your Profile or any other breach of security.* The MyGovID terms and Conditions[16] state: *You must* ***…*** *notify the ATO myGovID Help Desk on 1300 287 539 option 2 as soon as you suspect or become aware that the security of your myGovID account or myGovID credential has been compromised.* It will also be important for the OA to develop a detailed description of the fraud management solution for digital identity system participants that explains the key features, processes and underlying infrastructure. Openness and transparency for other digital identity system participants is also a key requirement.	**Recommendation G2: The Oversight Authority should publish a user guide to fraud management in the digital identity system to enhance consumer understanding and awareness.** The user guide could be in the form of an FAQ with information and links on how to report a suspicious transaction or other concerns regarding fraud.	**Action Required**
APP 2: Anonymity and Pseudonymity	Not Applicable		**-**

[15] Australia Post, *Digital iD™ Terms of Use* (13 July 2019) <digitalid.com/terms/web.html>.

[16] Australian Government, *myGovID Terms of use – User* (November 2019) <www.mygovid.gov.au/mygovid-terms-of-use-user>.

APP 3: Collection of solicited personal information	Both APP 3 and the TDIF contain rules on data minimisation and there is a commitment to this in various sections of the TDIF. Section 3.9 (Consent) of *TDIF4 04 Functional Requirements* include: *The Applicant MUST only disclose the Individual's Attributes required for the Relying Party's transaction with that Individual's Consent.* Section2.1 (Attribute Sets) of *TDIF4 06A Federation Onboarding Guidance* states: *The Attributes passed through the federation are split into Attribute sets. Attribute sets correspond to the logical sets of attributes that a RP will typically ask for as a collection, and that a user will provide consent for as a collection. Some attribute sets will contain a single attribute, and some will contain a number of attributes. The presence of attribute sets does not preclude attributes being requested individually by an RP to support the principle of only releasing the* ***minimum*** *attributes required.* Section 5.2 (Computed Attributes) of *TDIF4 06D Attribute Profile* states: *Using Computed Attributes supports privacy outcomes by only releasing the* ***minimum*** *required set of Attributes to RPs to meet the need of the service being accessed.* Section 3.9 (Privacy Considerations) of *TDIF4 06B OpenID Connect 1.0 profile* states: *Attributes are only to be shared in accordance with the Attribute Sharing Policy set out in the TDIF: 06 – Federation Onboarding Requirements. Data minimisation is an essential concept that underpins the Australian Government's identity federation. This is an important consideration in the design, for example, ensuring that only the* ***minimum*** *attribute set required to service the authentication request from a Relying Party is returned to the Identity Exchange from an Identity Service Provider.* The data minimisation requirement is not impacted by exceptions that may apply elsewhere (e.g., in APP 6 of the Privacy Act), so even when data is collected under legal authority the amount of data must still be minimised. Data minimisation requirements in APP 3 also apply to data *sharing* in many circumstances, as the sharing of data with a third party (e.g., in a data matching scenario) results in a new 'collection' by that third party. Additional data minimisation requirements are included in the TDIF. The data fields that may be collected or shared by specific TDIF accredited parties are set out in Section 3.6 (Attributes to be verified, validated and recorded) and Section 3.7 (Attribute disclosure) *of TDIF4 05 Role Requirements.* However, there is no compulsion in the TDIF requirements for some of these fields to be collected or shared, and only a small number of data fields MUST be shared by participants. There is a proposal for sharing some additional fields in exceptional circumstances – Refer to D. Restricted Attributes. In addition, some data may be collected from external sources (outside the digital identity system) for fraud management purposes. For example, a law enforcement agency might provide access to a list of known compromised identity documents that can then be used in the proposed fraud analytics engine. Data minimisation rules help to reduce the overall privacy and security risk profile of the digital identity system. Data minimisation also helps to build community support for the digital identity system, and the DTA has promoted the digital identity system as a privacy friendly approach to digital identity that does not require over-sharing of data. In the case of a specific investigation regarding fraud or suspicious transactions, data minimisation will be less of a concern than in the day-to-day running of the digital identity system. There will be greater clarity around the exact data fields required to complete the investigation, and the DTA (via responses to PIA1 and PIA2) has already flagged that some additional data may be shared for fraud investigations. However, a basic data minimisation test should still be applied to fraud investigations to prevent over-sharing. Some further guidance is provided below (refer to Section G4,B. Double Blind) on the types of information that should not be collected.	**Recommendation G3: In order to comply with the data minimisation requirements in APP 3 and the TDIF, the amount of information collected for fraud management purposes should be limited.** Some further guidance is provided below (refer to **Recommendations** G**9** and **G10** below) on the types of information that should not be collected.	**Action Required**
APP 4: Dealing with unsolicited personal information	Compliance with APP 4 is not impacted by the proposed fraud management solution in the digital identity system.		**Compliant**

APP 5: Notification	APP 5 sets out requirements for the notice to be given to applicants. These requirements are mirrored and slightly enhanced in sections 3.5 (Notification of Collection) and 3.9 (Consent) of *TDIF4 04 Functional Requirements* – which requires accredited parties to meet specific notice and consent rules. The Australia Post Digital iD Privacy Notice[17] states: *You hereby authorise us to disclose the information we hold about You and grant access to Your Profile to law enforcement and government authorities and agencies in accordance with their lawful requests.* The ATO myGovID Privacy Notice[18] states: *Your personal information is used to… investigate and verify the operation of the myGovID system.* *We may use your information to… identify and respond to issues that may indicate authentication integrity is at risk; and detect, investigate, and prosecute criminal offences.* Although these Notices are adequate, they could be enhanced by a specific notice that the double blind can be lifted for fraud investigations where the Privacy Notice or other product descriptions make specific reference to the double blind as a privacy enhancing feature.	**Recommendation G4: Where a TDIF participant makes a specific reference to the double blind as a privacy enhancing feature, their Privacy Notice must disclose that the double blind can be lifted for fraud management purposes.** This Recommendation may need to be implemented on a case-by-case basis, as not all TDIF participants refer to the double-blind arrangements.	**In progress**
APP 6: Use or Disclosure	APP 6 places restrictions on the use and disclosure of personal information. The TDIF Privacy Requirements place some additional restrictions on the use and disclosure of personal information.[19] Information could be used or disclosed for fraud prevention or fraud investigation under multiple exceptions to APP 6.[20] These options include: *6.2 (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is… related to the primary purpose (for non-sensitive information); or* *6.2 (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or* *6.2 (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.* APP 6.2 (a) is a useful option for using or disclosing data for fraud management activities, as managing identity fraud is related to the primary purpose (identity verification) and consumers are likely to reasonably expect this type of use. For example, identity fraud is highlighted as an issue in TDIF participant privacy policies, notices and terms and conditions and is also highlighted in the TDIF requirements: Section 3.7 of *TDIF4 04 Functional Requirements* states: ***3.7 Limitation on use of behavioural information*** *The Applicant MUST only collect, use and disclose information about an individual's behaviour on the identity federation to:* *(a) Verify the identity of an individual and assist them to get a service.* *(b)* ***To support identity fraud management functions.*** *(c) To improve the performance or usability of the Applicant's product,* *(d) To de-identify the data to create aggregate data.* APP 6.2 (b) is easy to trigger in the context of fraud investigation. For example, the *Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2018*[21] authorises collection, use and disclosure of personal information for**…** ***…*** *preventing, detecting, investigating or dealing with:*		**Compliant**

[17] Australia Post, *Digital iD™ Privacy Notice* (13 September 2019) <digitalid.com/privacy.html> and repeated in Australia Post, *Digital iD™ Terms of Use* (13 July 2019) <digitalid.com/terms/web.html>.

[18] Australian Government, *myGovID Privacy Notice* (May 2019) <www.mygovid.gov.au/mygovid-privacy-notice>.

[19] Refer to sections 3.6, 3.7, 3.8 and 3.9 of TDIF4 *04 Functional Requirements* (March 2020).

[20] <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

[21] Part VIID—Collecting, using and disclosing personal information that may be relevant for integrity purposes – Section 86B Simplified outline of this Part <www.legislation.gov.au/Details/C2018A00075>.

	(a) serious misconduct by persons working for Commonwealth bodies; or *(b) fraud affecting Commonwealth bodies; or* *(c) offences against Chapter 7 of the Criminal Code (which is about the proper administration of Government).* *The authorisation is relevant to laws (such as privacy laws) that limit the collection, use and disclosure of personal information unless authorised by law.* APP 6.2 (e) is a useful option for facilitating the investigation of fraud or suspicious transactions where an enforcement body is involved. Finally, consent may also play a role in allowing data to be shared for investigating fraud, as some investigations are likely to be triggered by consumer requests.		
APP 7: Direct Marketing	**Not applicable** – Section 3.6 (Collection and use limitation) of *TDIF4 04 Functional Requirements* prohibits direct marketing.		**–**
APP 8: Cross Border Disclosure	Compliance with APP 8 is not impacted by the proposed fraud management solution in the digital identity system.		**Compliant**
APP 9: Government Related Identifiers	APP 9 places some restrictions on the use of government related identifiers by organisations. These requirements might potentially apply to some **private sector** IdPs and Relying Parties. The TDIF Privacy Requirements also include a specific restriction on government related identifiers: *The Applicant MUST NOT create a new government identifier for use across the identity federation (i.e., an identifier that is sent to more than one Relying Party or Identity Service Provider).*[22] The TDIF requirement is stricter than APP 9 and has been included in order to prevent the development of a national identifier (either deliberately or accidentally). Importantly, the TDIF Attribute Profile does not allow the unique identifier created by an IdP for its clients to be shared with RPs in the day-to-day business of the TDIF. This is because the 'double blind' arrangements are designed to restrict RP knowledge of the IdP chosen by clients (and vice versa). Any sharing of unique IdP identifiers would obviously undermine this arrangement. However, exceptions are allowed where there is an investigation of a suspicious transaction or identity fraud. It is important that this exception is reserved for special circumstances and does not become the norm. The issue of identifiers is relevant to both APP 6 and APP 9, as APP 6 (and its TDIF equivalent) may also restrict the disclosure of some identifiers in the digital identity system.		**Compliant**
APP 10: Quality of Personal Information	APP 10 requires agencies to ensure that data is accurate and up to date in relation to the purpose for which it is collected and used. The TDIF Privacy Requirements mirror APP 10, with some additional requirements for IDPs. Compliance with APP 10 is not impacted by the proposed fraud management solution in the digital identity system.		**Compliant**

[22] Refer to Section 3.11 (Government Identifiers) of *TDIF4 04 Functional Requirements* (March 2020).

APP 11: Security	APP 11 sets a somewhat vague standard for ensuring security of personal information. The TDIF contains a range of more specific security requirements and security audit requirement, in Section 4 (Protective Security Requirements) and Section7 (Functional Assessments) of *TDIF4 04 Functional Requirements (March 2020)* and references to security considerations in other key sections of the TDIF documentation. APP 11 states that security measures should be in proportion to the risk of the information being disclosed. The sharing of some additional data for fraud investigations may lead to a small rise in the risk profile of TDIF, as more data will be shared, and some of this data (if it fell into the wrong hands following a breach) might lead to increased security risks for individuals. The following three measures available may help to reduce / manage this increased security risk: ● **Measure 1:** Security reviews ● **Measure 2:** Reducing the amount of data collected and stored ● **Measure 3:** Reducing the data retention period for stored data Addressing these measures are reflected in the following recommendations.		
APP 11: Security	**Measure 1: Security reviews** The fraud management process for the digital identity system is initially being developed as a Proof of Concept (PoC) by Services Australia. When a mature system is developed it should be subject to an independent security review. TDIF accredited participants are already required to undertake regular security reviews. The proposed fraud management solution should be the subject of an independent security review (either as a stand-alone review or as part of a scheduled review).	**Recommendation G5: The digital identity system fraud management solution should be subject to an independent security review.**	**Action Required**
APP 11: Security	**Measure 2: Reducing the amount of data collected and stored** Reducing the amount of data collected will also help to manage the security risk profile of the fraud solution, as it reduces opportunities for breaches involving large amounts of data. This issue is already addressed under consideration of APP 3 above.	Refer to Recommendation G3.	**Action Required**
APP 11: Security	**Measure 3: Reducing the data retention period for stored data** TDIF PIA2 stated: ***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**.* We have been informed that some fraud related data will need to be retained for a lengthy period to assist with investigations and enforcement. It may also be useful to retain fraud related data for a lengthy period so that it can be analysed for trends and vulnerabilities. However, in this second situation, it may be possible to de-identify some of the data.	**Recommendation G6: The digital identity system fraud management solution should be subject to a formal data retention policy that requires data to be destroyed once it is no longer required for investigations, enforcement or further analysis. In some cases it may be appropriate to de-identify the data.**	**Action Required**
APP 12: Access	In addition to the usual access provisions set out in APP 12, the TDIF includes an additional mandatory access requirement for the Exchange: ***3.12.3 Individual history log*** *The Applicant MUST provide Individuals with a centralised view of the metadata of services the Individual accessed, the time of access and the Attributes passed to the Relying Party unless such information has already been destroyed by the Applicant in accordance with the TDIF.*[23] The proposed use of digital identity system related data for fraud prevention and the investigation of fraud does not raise new or specific concerns regarding access and compliance with APP 12 or the TDIF access requirements.		**Compliant**
APP 13: Correction	Compliance with APP 13 is not impacted by the proposed fraud management solution in the digital identity system.		**Compliant**

[23] Refer to section 3.12.3 (Individual history log) of TDIF4 *04 Functional Requirements* (March 2020).

Governance: Consultation	The proposed use of digital identity system related data for fraud management and the investigation of fraud may have an impact on a wide range of stakeholders. The DTA already has consultations scheduled with key parties for the next PIA of the digital identity system and for the development of the legislative package that is being developed to support the digital identity system – rather than establish a separate consultation process, fraud management issues should be covered in the scheduled consultation rounds.	**Recommendation G7: Include fraud management issues in the scheduled stakeholder consultation rounds (such as consideration of the legislative package).**	**Action Required**
Governance: Managing Function Creep	Privacy regulators and consumer stakeholders have consistently expressed concern about the potential for function creep in the digital identity system. Managing concerns about function creep in the context of fraud management is going to be challenging, as any attempt to lift the double blind weakens a key privacy design feature of the digital identity system, although these concerns can be lessened if the circumstances are tightly constrained and managed. Function creep can be difficult to prevent, but some measures are available that might help to manage it: **Measure 1: Define and restrict the exact categories of fraud that may trigger lifting the double blind** The digital identity system fraud documentation could be enhanced by a set of specific definitions of key terms like 'fraud' and 'suspicious transaction' that will help to assure stakeholders that the double blind is only being lifted in response to serious issues related to system integrity. **Measure 2: Establish regular reviews of the fraud management system** The digital identity system fraud management solution should be subject to regular reviews (e.g., every three years) complemented by annual reporting (e.g., statistical data and case studies on instances of fraud). **Measure 3: Conduct a Privacy Impact Assessment (PIA) on the fraud analytics process** The digital identity system fraud management proposal includes an analytics engine that to outsiders appears to be a 'black box'. The inner workings of the system are unknown, and it may be difficult to publish information about the analytics engine without compromising efforts to detect fraud. However, stakeholders will gain confidence about the system if it is subject to a PIA, where the information sources and flows can be analysed by an independent reviewer.	**Recommendation G8: Steps should be taken to manage concerns regarding function creep in relation to fraud management.** These should include: – **Measure 1:** Define and restrict the exact categories of fraud that may trigger lifting the double blind – **Measure 2:** Establish regular reviews of the fraud management system **– Measure 3:** Conduct a Privacy Impact Assessment (PIA) on the fraud analytics process	**Action Required**

G4. Potential impact on key TDIF privacy features

In addition to the analysis of APP / TDIF privacy compliance in above, we have examined the potential impact of the proposed fraud management solution on key privacy features of the digital identity system.

There are three key privacy features that have been promoted for the digital identity system:

A. Federated / Distributed Model
B. Double Blind
C. Voluntary Participation

A. Federated / Distributed Model

A key privacy feature of the TDIF is that a federated / distributed model has been developed, rather than a centralised model.

In practice, TDIF allows multiple IdPs to operate (and two IdPs have been accredited). This reduces potential privacy impacts because there is no single, central store of identity information in the TDIF.

However, if a fraud management solution effectively collects all of the distributed identity information and stores it in a central data store, then this would undermine the value of the distributed / federated model.

Fortunately, the proposed fraud management for the digital identity system relies on the exchange of specific data between parties in response to a request or an investigation. The solution does not require the creation of a new or centralised store of all digital identity system data (that would otherwise be distributed across multiple participants).

Over time a small amount of digital identity system data related to specific investigations will be retained by the fraud management system. This will play an important role in identifying trends and vulnerabilities, without having a significant impact on the overall protection of privacy. This privacy guidance has recommended that this data should be deleted or de-identified in accordance with a formal data retention policy.

B. Double Blind

A key privacy feature of the digital identity system is that participants are deliberately 'blinded' as to the source of identity data and the use of identity data. This is achieved by the intervention of an Identity Exchange. In the normal day to day activities of the digital identity system an IdP will not know where a digital identity is being used, and a relying party will not know which IdP has provided a User with their digital identity. This system addresses privacy concerns that have plagued previous digital identity proposals (such as Gatekeeper PKI) which left comprehensive trails of how a consumer acquired and used their digital identity – allowing a detailed consumer profile to build up over time.

However, if a fraud management solution collected all of the distributed transactional information and stored it in a central dataset, then this would reduce the protection offered by the Double Blind.

The two-prior independent PIAs on the TDIF both noted that the double blind could be lifted in some exceptional circumstances, including the investigation of fraud or a suspicious transaction, but it was stressed in PIA2 (2018) that:

> *it is intended that this type of access will be rare, and will not lead to widespread surveillance or monitoring*

The proposed fraud management solution does pose some risks to the maintenance of the double blind, and there is a possibility that confidence in TDIF privacy protections will reduce if the circumstances in which the double blind can be lifted are not severely restricted.

Galexia has developed two important and linked recommendations on this issue:

Recommendation G9: The double blind can be lifted for fraud management purposes where one of three key conditions are met:

1) Where information needs to be obtained from participants in the digital identity system to investigate suspected fraud or to assist with enforcement;

2) Where information regarding a known fraud needs to be shared with other digital identity system participants; or

3) Where the digital identity system is subject to a cyber security incident that cannot be managed without lifting the double blind.

Note: Recommendation G9 is closely tied to Recommendation G8 (Measure 1) – as the definitions of key terms such as fraud need to be clarified so that this type of access will remain rare.

Recommendation G10: The double blind should not be lifted for the following purposes:

1) To automatically check **all** identities or **all** transactions against specific criteria (e.g., checking across the entire ecosystem against a central list of safe or compromised identities or other particulars); or

2) To profile the behaviour of individuals.

Recommendation G10 is not a completely stand-alone restriction – it needs to be read closely with Recommendation G9.

- For example, if the double blind is lifted for an investigation in compliance with Recommendation G9, then any **relevant** information collected by the fraud management solution can be shared with **relevant** participants.
- This is despite the broader restriction proposed in Recommendation G10 – which is intended to restrict the automatic collection of all data in the digital identity system under the general banner of ‘preventing fraud’.

C. Voluntary Participation

A key privacy feature of the digital identity system is that participation is voluntary.

The proposed fraud management solution does not have a direct impact on the voluntary nature of the digital identity system.

G5. Overall Finding

Whilst recognising security concerns, stakeholders have a broad spectrum of strongly held concerns and identify this as a pivotal issue. Some concerns include:

- Creation of exemptions to lift the ‘double blind’ is a weakening of the TDIF and an example of function creep
- Definition of fraud – as opposed to a ‘suspicious transaction’
- Requiring the fraud investigator be subject to investigation by the OA – and indeed a separation requirement between fraud investigations and the OA
- Establishing strict protocols (even judicial oversight)

A fraud management solution for the digital identity system will need to be carefully constrained and managed so that it does not have a negative impact on trust and confidence in the digital identity system. In particular, the core activities of the fraud management solution should be limited to the investigation and management of clearly defined categories of fraud in limited circumstances, and the key privacy design features of the digital identity system should be preserved.

H. Data Retention Periods: A policy decision on data retention periods (and processes) for key data sets.

H1. Proposal Overview: To retain some personal data collected in the Digital Identity system.

DTA is proposing to retain some personal information collected in the Digital Identity system until it is no longer required for a business purpose.

This may include some meta data collected by the Identity Exchange and some more detailed data collected by the Oversight Authority's fraud management function during investigations.

H2. Solution Overview: To develop a formal Records Authority for the Digital Identity system, including time limits.

To manage this issue DTA is working with the National Archives to develop a formal Records Authority for the Digital Identity system.

The Records Authority would apply to information collected by the Identity Exchange and the Oversight Authority. (Identity Providers and Relying Parties are generally covered by existing Records Authorities).

The Records Authority would include time limits beyond which data would need to be destroyed or de-identified.

H3. Findings and Recommendations

The earlier PIAs have made a number of findings and recommendations about data retention.

In PIA1 (2016), stakeholders indicated the potential measure of most interest to mediate concerns about meta-data was the **development of a very short retention period for the meta-data** – the view being that a short retention period may minimise the amount of data stored, therefore reducing the attractiveness of the data as a target for surveillance or external attack, and reducing the impact of any disclosure or breach. The DTA stated that a major driver for retaining the meta-data is to facilitate the investigation of identity fraud and suspicious transactions and the DTA agreed that further research on how long meta-data needs to be retained for the purpose of investigating identity fraud might help to determine an appropriate data retention period. The following recommendation was made:

> ***Recommendation 3:* The Identity Exchange and the retention of metadata**
> *DTA should conduct further research on the period that meta-data needs to be retained in order to facilitate the investigation of identity fraud and suspicious transactions. This period should then be 'balanced' against the privacy risks and impacts of retaining the data, and an appropriate data retention period should be incorporated into the design of the Identity Exchange. For the avoidance of doubt, an 'appropriate period' could be shorter than the period required for all investigative purposes.*

In PIA2 (2018) it was found that there were ongoing stakeholder concerns in relation to the collection, use and disclosure of metadata by the Identity Exchange – as this can have a negative impact on key privacy issues (such as function creep and the potential use of TDIF data for surveillance and monitoring). The PIA noted ongoing concert about retention periods and made a further recommendation:

> ***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.*

In its response to this recommendation in PIA2, the DTA flagged it as an area requiring further exploration:

> 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 (i.e., 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.

During consultations on the proposed solution, stakeholder raised the following concerns:

- Opportunities for unlawful access and breach of retained data;
- Not setting a time period for deletion increases the risk;
- Unsafe to retain meta-data unless it is impossible to be used to re-identify that meta-data or any other data. Amplified by concerns around re-identification risk and that destroying data is the best protection against re-identification;
- Archiving transaction data should not be permitted – as a general proposition;
- The current proposal to develop a Records Authority seems 'open ended'; and
- 'Business purpose' must be defined very explicitly.

Stakeholder suggested some specific requirements that could strengthen the proposed solution, including:

- Establishment of adequate cybersecurity preventative measures;
- Establishment of a time period for deletion;
- Ensuring data is destroyed once it is no longer needed for the purpose of providing identity services;
- Developing a clear and explicit definition of 'business purpose'. Notify Users of these purposes; and
- Establishing clear legislative protections against secondary use.

The combination of the recommendations in the previous PIAs and the ongoing stakeholder concerns mean that this is now an issue that requires urgent attention by the DTA.

Recommendation H1: The DTA should develop a formal policy position with strict time limits for the retention of TDIF transaction data related to an individual's transactions in the Exchange. This could include a formal Records Authority. The policy position should explicitly restrict the retention of data to purposes required for digital identity services.

Appendix 1 – Summary of the changes made to the APPs in the TDIF Functional Requirements

A useful reference is a mapping of the of the APPs to the TDIF4 Privacy Requirements – and identifying how the TDIF requirements may extend the APPs:

Summary of the changes made to the APPs in the TDIF Functional Requirements

Australian Privacy Principle (APP)	TDIF4 Functional Requirement	Nature of change	Details
APP 1: Open and Transparent Management of Personal Information	3.2 Privacy governance	**Consistent for all parties**	Removed distinctions between government agencies and private sector organisations
APP 2: Anonymity and Pseudonymity	–	**Not included**	
APP 3: Collection of solicited personal information	3.6 Collection and use limitation 3.7 Limitation on use of behavioural information 3.8 Collection and disclosure of biometrics	**Strengthened**	New limitations on collection Specific requirements for biometrics data
APP 4: Dealing with unsolicited personal information	–	**Not included**	
APP 5: Notification	3.5 Notification of Collection	**Equivalent**	
APP 6: Use or Disclosure	3.6 Collection and use limitation 3.7 Limitation on use of behavioural information 3.8 Collection and disclosure of biometrics 3.9 Consent	**Strengthened** **Made consistent for all parties**	New limitations on secondary use Specific requirements for biometric data
APP 7: Direct Marketing	3.6 Collection and use limitation	**Strengthened**	Complete prohibition
APP 8: Cross Border Disclosure	3.10 Cross border and contractor disclosure of Personal Information	**Clarified**	Narrowed compliance options and restricted use of data
APP 9: Government Related Identifiers	3.11 Government Identifiers	**Strengthened**	Completely new requirements and prohibitions
APP 10: Quality of Personal Information	3.13 Quality of personal information	**Equivalent**	
APP 11: Security	4 Protective Security Requirements 3.15 Destruction and de-identification	**Strengthened**	Completely new requirements
APP 12: Access	3.12 Access, correction and individual history log	**Made consistent for all parties**	Removed distinctions between government agencies and private sector organisations
APP 13: Correction	3.12 Access, correction and individual history log	**Made consistent for all parties**	Removed distinctions between government agencies and private sector organisations

Appendix 2 – Trusted Digital Identity Framework (TDIF) Policies and Standards – Privacy Requirements updates from TDIF3 (March 2019) to TDIF4 (March 2020)

This PIA considers the range of changes to privacy requirements of the TDIF. While it was important for the PIA process to consider the details and reasons for changes as PIA2 (September 2018) covered TDIF3 (March 2019) and Galexia developed resources to assist with understanding the subsequent changes in TDIF4 (March 2020).

Our experience with this process shaped Recommendation 33: Document changes to the TDIF and consider and communicate possible privacy impacts in Section 32 of this PIA.

A. DTA published updates to the TDIF Privacy Requirements – Stakeholder and Community Feedback Updates

The DTA has released a number of TDIF policy drafts for consultation and included some comments about changes for each TDIF release. We have extracted the relevant changelog specific to the privacy requirements and have found this useful to broadly understand scope of changes in each TDIF release.

TDIF (Component 1) – February 2018[24]

1.7 Privacy Requirements

- *The document Core Privacy Requirements has been renamed Privacy Requirements.*
- *The document formally titled Privacy Audit has been merged with the Privacy Requirements.*
- *The document now aligns with the Australian Government Agency Privacy Code for conducting Privacy Impact Assessments.*
- *Privacy Impact Assessments are now required where an Applicant identifies a high privacy risk.*
- *The Office of the Australian Information Commissioner (OAIC) has been removed as a stakeholder to whom data breaches are to be reported. This change was required as the OAIC may not be able to action some data breaches where the Applicant is not operating within the jurisdiction of the OAIC.*
- *The uses and disclosures section of the document now makes a distinction between verification events (i.e., where consent is required), direct marketing (not allowed) and other uses and disclosures (which must comply with the Privacy Act).*
- *The document now aligns with the Privacy Act 1988 in relation to access and correction.*
- *It is now clearer in the document that the Approved Assessor undertaking the privacy audit is required to be independent of the identity service under review.*

[24] <dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-stakeholder-and-community-feedback.pdf>

TDIF (Component 2) – August 2018[25]

1.6 Interim Memorandum of Agreement

- *The System Governance Interim MOU (MOU) consolidates the Federation Deed and MOU, and the Interim Accreditation Governance document, into one document. (The Federation Deed and MOU, and the Interim Accreditation Governance document, were each included in TDIF release two). This approach streamlines the governance arrangements for the System ('System Governance') during the roll-out of pilot services from October.*
- *The MOU provides for the DTA to act as an 'Oversight Authority' for the System and outlines the rights, powers and obligations of that Oversight Authority to ensure the safe, reliable and effective operation of the System. The TDIF MOU document previously referred to an 'Accreditation Authority', which was a body that had responsibility for accrediting participants within the System – the Oversight Authority has broader responsibility for administration and enforcement of arrangements for the System.*
- *The MOU sets out the roles and responsibilities of each participant within the System to ensure accountability and certainty within the System, and to ensure that use of the System is consistent with the requirements of the TDIF.*
- *The MOU is an interim arrangement which is designed to 'fall away' as the scope of the System expands, and other non-Commonwealth participants seek to use the System (the MOU will be replaced by 'Operating Rules' in due course). In the meantime, it has flexibility for other Commonwealth entities to participate in the system (for example, as a Relying Party as new services are on-boarded).*
- *The MOU requires the Identity Exchange to maintain the privacy of the System through the 'double-blind' mechanism and the legal structure of this document (including the obligations of the participants) reflects the double-blind technical architecture. The MOU also enshrines other privacy requirements – for example, the Oversight Authority must notify the Privacy Commissioner of proposed changes to the TDIF and invite comment on those changes.*

1.8 Overview and Glossary [selected 3 out of 10]

- *Added a description of 'double blind' in the objectives and how this will be achieved.*
- *Removed ambiguity about the number of identity exchanges that will operate in the identity federation over time (there will likely be several).*
- *Introduced the concepts of the Oversight Authority and Operating Rules and added some of their roles and responsibilities.*
- *Added and updated a number of glossary terms that were missed from the first TDIF release.*

TDIF (Component 3) – April 2019[26]

1.8 Privacy Requirements

- *Added a section on limitation of use and disclosure of behavioural information to Identity Service Providers so they do not use data collected from the services beyond providing and improving the service and detection and investigation of fraud.*
- *Streamlined consent section so not to duplicate common law requirements.*
- *Revision of overseas and contractor disclosure section so it better maps to APP 8.*

[25] <dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Trusted%20digital%20identity%20framework%202/Stakeholder%20and%20Community%20Feedback%20Summary%20from%20August%202018.pdf>

[26] <dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-component-3-stakeholder-community-feedback-summary.pdf>

TDIF Release 4 May 2020, version 1.0[27]

1. Summary of changes

The fourth TDIF release resulted in a complete overhaul of the framework. Key changes include:

- *Two new Identity Proofing Levels were added to support the commercial sector who may have slightly different identity proofing needs than those of government agencies.*
- *Biometric verification requirements.*
- *The TDIF Accreditation Process was expanded to support Applicants that undergo TDIF Accreditation and do not join the Australian Government's identity federation.*
- *The removal of SHOULD requirements.*
- *The introduction of unique numbering for every TDIF requirement and applicability indicators.*
- *Requirements were separated from guidance.*

B. Broad mapping of changes in requirements documents from TDIF3 to TDIF4

The fourth TDIF release resulted in a complete overhaul of the framework.

TDIF Release 3	TDIF Release 4 (March 2020)
Overview and Glossary	**01 Glossary** – includes a list of acronyms and defines the key abbreviations and terms used in the TDIF. **02 Overview** – high-level overview of the TDIF
Accreditation Process	**03 Accreditation Process** – sets out the process and requirements an Applicant is required to complete to achieve TDIF accreditation.
Fraud Requirements	**04 Functional Requirements** – outlines requirements applicable to the Accredited Roles, including fraud control, privacy, protective security, user experience and technical testing. It also includes a series of Functional Assessments to be undertaken by the Applicant to achieve TDIF accreditation including a Privacy Impact Assessment, Privacy Assessment, Security Assessment, penetration test and an Accessibility Assessment against the Web Content Accessibility Guidelines.
Privacy Requirements	
ProtSec Requirements	
UX Requirements	
Technical Requirements	
ProtSec Reviews	
Identity Proofing Requirements	**05 Role Requirements** – includes user terms and lifecycle management requirements applicable to the Accredited Roles.
Authentication Requirements	
Risk management Requirements	Removed – Risk is now part of Fraud, Protective Security and Privacy Requirements in 04 Functional Requirements.
Technical Requirements	**06 Federation Onboarding Requirements** – outlines the requirements to be met when an Applicant's identity system is approved to onboard to the Australian Government's identity federation. This document includes functional requirements, technical integration testing requirements, operating obligations and the accreditation requirements for an Identity Exchange.
Architecture Overview	**06A Federation Onboarding Guidance** – provides guidance to Applicants on meeting requirements set out in the 06 Federation Onboarding Requirements.
OpenID Connect Profile	**06B OpenID Connect Profile** – describes how OpenID Connect 1.0 is used within the Australian Government's identity federation.
SAML Profile	**06C SAML Profile** – describes how SAML 2.0 is used within the Australian Government's identity federation.
Attribute Profile	**06D Attribute Profile** – describes the Attributes used within the Australian Government's identity federation and how these are mapped in the OpenID Connect 1.0 Profile and SAML 2.0 Profile.

[27] <dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-framework-4-final/TDIF%20-%20Stakeholder%20and%20Community%20Feedback%20-%20Release%204%20Final.pdf>

C. Analysis and Traceability Matrix – Mapping Changes from TDIF4 to TDIF3

PIA3 considered the September 2018 version of Release 3 of the TDIF.

Following this, after a period of internal review and external stakeholder consultation, the DTA published Release 4 of the TDIF in April 2020.[28]

While a detailed change log between TDIF3 and TDIF4 was not available and consideration of the effect of individual changes and the overall package was complex, Galexia developed a detailed comparison table to assist with the analysis and development of the PIA. For brevity in the public release of the PIA, more detailed commentary and findings has been removed by Galexia.

This PIA considers changes to the TDIF Privacy Requirements – we have not undertaken a comprehensive analysis of changes in other requirements, guidelines or profiles.

The Table below the Privacy Requirements in *TDIF4 04 Functional Requirements* to the *TDIF3 Privacy Requirements*.

While we have not made a specific recommendation about the impact of changes, we have made a recommendation about improving the traceability and justification of changes to privacy aspects of the TDIF and digital identity system. As part of this, we do suggest a response from DTA to some of the areas that may have changed – and we recognise some of these changes may have been unintentional or drafting related, but the basis of these changes will be useful for openness and transparency. Refer to Recommendation 33: Document changes to the TDIF and consider and communicate possible privacy impacts.

Galexia mapping Privacy Requirements from TDIF4 to TDIF 3	
TDIF Release 4, *04 Functional Requirements* (Mar 2020, version 1.0) – Section 3 Privacy Requirements	**TDIF Release 3, *Privacy Requirements* (Mar 2019, version 1.2)**
3.1 General privacy requirements	**2.1 General requirements** Identity Exchanges MUST operate separately from other identity federation participants and MUST establish and maintain its own privacy management arrangements.
TDIF Req: PRIV-03-01-01; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST comply with its obligations under the Privacy Act, including the Australian Privacy Principles (APPs), and Australian Government Agencies Privacy Code or, where relevant, state or territory privacy legislation.	The Applicant MUST comply with its obligations under the Privacy Act or, where relevant, state or territory privacy legislation and applicable Privacy Codes.

[28] Digital Transformation Agency, *The Trusted Digital Identity Framework (TDIF) Documents* (Release 4, April 2020) <www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework/framework-documents>

TDIF Req: PRIV-03-01-02; Updated: Mar-20; Applicability: A, C, I, X If the Applicant is a small business operator as defined by the Privacy Act, and therefore exempt from the Privacy Act, it MUST opt-in to coverage of the APPs as an organisation. **TDIF Req: PRIV-03-01-03;** Updated: Mar-20; Applicability: A, C, I, X Any state or territory government Applicant not covered by state privacy laws or not prescribed under s6F of the Privacy Act 1988 MUST comply with APPs for the purpose of achieving and maintaining TDIF accreditation.	If the Applicant is a small business operator as defined by the Privacy Act, and therefore exempt from the Privacy Act, it MUST opt-in to coverage of the APPs as an organisation. Any state or territory government Applicant not covered by state privacy laws providing substantially the same level of protection as the APPs MUST comply with APPs for the purpose of achieving TDIF Accreditation.
–	For the purpose of TDIF accreditation, an Applicant MUST protect the greater subset of: • ‘Personal information’ as defined by the Privacy Act. • Information about an individual who has died. • Where the Identity Service Provider is a state or territory government agency, personal information as defined by a relevant state jurisdiction. • The data created and retained about the attributes disclosed by an Identity Exchange.
–	The following privacy requirements apply to all Applicants unless explicitly stated otherwise. There are some requirements on Privacy Assessors under the heading Privacy Audit.
3.2 Privacy governance	**2.2 Privacy governance**
3.2.1 Privacy roles **TDIF Req: PRIV-03-02-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST have at least one designated Privacy Officer who is the primary point of contact for advice on privacy matters. **TDIF Req: PRIV-03-02-01a;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate how the following Privacy Officer functions are carried out: a) Handling of internal and external privacy enquiries and complaints. b) Handles requests for access to and correction of Personal information. c) Maintaining a record of Personal information holdings. d) Assisting with the preparation of Privacy Impact Assessments (PIAs). e) Maintaining a register of PIAs. f) Measuring and documenting performance against the Privacy Management Plan and reviewing and, where relevant updating, the Privacy Policy at least annually relevant to the TDIF.	**2.2.1 Roles** The Applicant MUST: • Have at least one designated Privacy Officer. • Ensure Privacy Officers are the primary point of contact for advice on privacy matters. • Ensure that the following Privacy Officer functions are regularly carried out: o Handling of internal and external privacy enquiries, privacy complaints. o Requests for access to and correction of personal information made under these Privacy Requirements and privacy legislation. o Maintaining a record of the Accredited Providers personal information holdings. o Assisting with the preparation of Privacy Impact Assessments (PIAs). o Maintaining the Applicant’s register of PIAs. o Measuring and documenting the Applicant’s performance against the privacy management plan and updating privacy policies, at least annually.

TDIF Req: PRIV-03-02-02; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST have at least one designated Privacy Champion. **TDIF Req: PRIV-03-02-02a;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate how its Privacy Champion promotes a culture of privacy that values and protects Personal information. **TDIF Req: PRIV-03-02-02b;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate how its Privacy Champion approves its Privacy Management Plan, and reviews of the Applicant's progress against the Privacy Management Plan.	• At all times, have a designated Privacy Champion responsible for: o Promoting a culture of privacy within the Applicant that values and protects personal information. o Providing leadership within the Applicant's organisation on broader strategic privacy issues. o Reviewing and approving the Applicant's privacy management plan, and documented reviews of the Applicant's progress against the privacy management plan. o Providing regular reports to the Applicant's executive, including about any privacy issues arising from the Applicant's handling of personal information. An Applicant's designated Privacy Officer MAY also be its designated Privacy Champion.
3.2.2 Privacy Policy **TDIF Req: PRIV-03-02-03;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST publish a clearly expressed and up to date Privacy Policy about the management of Personal information by the entity. **TDIF Req: PRIV-03-02-03a;** Updated: Mar-20; Applicability: I, X The Applicant MUST have a separate Privacy Policy in relation to its identity system to that of its other business, organisation functions or Accredited Roles. **TDIF Req: PRIV-03-02-03b;** Updated: Mar-20; Applicability: I, X The Applicant MUST maintain separate Privacy Policies for their Identity Service Provider and Identity Exchange if they are accredited in both roles (i.e., a Privacy Policy for their Identity Service Provider and a separate Privacy Policy for their Identity Exchange). **TDIF Req: PRIV-03-02-04;** Updated: Mar-20; Applicability: A, C, I, X The Applicant's Privacy Policy MUST include information on: a) The kinds of Personal information that the entity collects and holds. b) How the entity collects and holds Personal information. c) The purposes for which the Applicant collects, holds, uses and discloses Personal information. d) How an Individual can access Personal information about themselves that is held by the Applicant and how to seek the correction of such information. e) How an Individual can complain about a breach of the APPs (or a particular jurisdiction privacy principle) and how the Applicant will deal with such a complaint. f) Whether the Applicant is likely to disclose Personal information to overseas recipients and if so the countries in which such recipients are likely to be located (if it is practicable to do so).	**2.2.2 Policies** An Applicant that is an IdP or Exchange MUST have a separate privacy policy to that of its other business or agency functions. The Applicant MUST publish a clearly expressed and up to date Privacy Policy about its management of personal information which MUST contain: • The kinds of personal information that the entity collects and holds. • How the entity collects and holds personal information. • The purposes for which the entity collects, holds, uses and discloses personal information. • How an individual may access personal information about the individual that is held by the entity and seek the correction of such information. • How an individual may complain about a breach of the APPs3 and these Privacy Requirements and how the entity will deal with such a complaint. • Whether the entity is likely to disclose personal information to overseas recipients and if so the countries in which such recipients are likely to be located (if it is practicable to do so).
TDIF Req: PRIV-03-02-05; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST review its Privacy Policy at least annually and update as necessary.	Privacy Policies MUST be regularly (at least annually) reviewed and updated.

3.2.3 Privacy Management Plan **TDIF Req: PRIV-03-02-06;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST develop and maintain a Privacy Management Plan that identifies measurable privacy goals and targets for its identity system and the practices, procedures and systems that will be implemented to achieve these targets and goals. **TDIF Req: PRIV-03-02-07;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST measure and document its performance against the Privacy Management Plan relevant to TDIF at least annually.	The Applicant MUST: • Develop and maintain a privacy management plan which identifies specific, measurable privacy goals and targets; and sets out how an Applicant takes steps as are reasonable in the circumstances to implement practices, procedures and systems to implement these Privacy Requirements and other relevant privacy laws. • Document the Applicant's performance against its privacy management plan at least annually.
3.2.4 Privacy awareness training **TDIF Req: PRIV-03-02-08;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST on an annual basis, provide privacy awareness training which incorporates these TDIF privacy requirements, to all Personnel that access the Applicant's identity system. A copy of these training materials will be requested by the DTA as part of initial accreditation and annually thereafter as part of the Annual Assessment. **TDIF Req: PRIV-03-02-09;** Updated: Mar-20; Applicability: A, C, I, X The privacy awareness training provided by the Applicant, MUST cover the Applicant's Privacy Policy and include the TDIF privacy requirements.	**2.2.3 Internal privacy capability** The Applicant MUST: • Include appropriate privacy education or training in any staff induction program it provides to staff involved in the Accredited Provider. The privacy education must address the privacy obligations of staff, and policies and procedures relating to privacy, particularly these Privacy Requirements. • Provide appropriate privacy education or training annually to all staff who have access to personal information in the course of performing their duties as a staff member related to the Applicant's role(s) in the identity federation. • Regularly review and update its privacy practices, procedures and systems, to ensure their currency and adequacy for the purposes of compliance with these Privacy Requirements and privacy laws. • Monitor compliance with its privacy practices, procedures and systems regularly.
3.3 Privacy Impact Assessment Further information on the PIA is outlined in Section 7.1. **TDIF Req: PRIV-03-03-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST maintain a register of the PIAs it conducts. **TDIF Req: PRIV-03-03-01a;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST publish the register, or a version of the register, on its website.	**2.3 Privacy Impact Assessment** [Note: The main component of Section 2.3 is extracted text below against Section 7.1 (TDIF4)] **…** • SHOULD publish the above mentioned PIAs, or a summary version or an edited copy of the PIA, on its website. **…**

3.4 Data Breach Response Management **TDIF Req: PRIV-03-04-01;** Updated: Mar-20; Applicability: A, C, I, X An Applicant, covered by the Privacy Act, MUST report eligible data breaches to affected individuals and the Information Commissioner as required under the Privacy Act and also report the eligible data breach to the Oversight Authority and DTA. **TDIF Req: PRIV-03-04-01a**; Updated: Mar-20; Applicability: A, C, I, X An Applicant, not covered by the Privacy Act, MUST report eligible data breaches as defined in the Privacy Act 1988 to affected individuals and the Oversight Authority and DTA. **TDIF Req: PRIV-03-04-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST develop and maintain a Data Breach Response Plan that includes a description of the actions to be taken if a breach is suspected, discovered, or reported by Personnel or external party, including a clear communication plan and information about when it is to be escalated to the data breach response team or third party. **TDIF Req: PRIV-03-04-03;** Updated: Mar-20; Applicability: A, C, I, X The Data Breach Response Plan MUST: a) List the roles or members of the response team. b) List the actions the response team is expected to take. c) Describe how the actions and roles in the plan align to the Applicant's Incident Response Plan.	**2.4 Data Breach Response Management** The Applicant MUST: • Have a documented Data Breach Response Plan (see below). • For Applicants covered by the Privacy Act 1988, report eligible data breaches to individuals and the Information Commissioner as required under the Privacy Act 1988 and also report the eligible data breach to the TDIF Accreditation Authority. • For Applicants not covered by the Privacy Act 1988, report eligible data breaches to individuals as described in the Privacy Act 1988 and also report the eligible data breach to the TDIF Accreditation Authority. The Data Breach Response Plan is a tool to help Applicants prepare for a data breach. It MUST, at a minimum, include: • The actions to be taken if a breach is suspected, discovered or reported by a staff member, including a clear communications plan and information about when it is to be escalated to the data breach response team (response team). • The members of the response team. • The actions the response team is expected to take. • Information about how the actions and roles in the plan relates to the Applicant's Incident Response Plan
3.5 Notification of Collection **TDIF Req: PRIV-03-05-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST notify or make people aware as required by APP 5.	**2.5 Notice of Collection** The Applicant MUST, when it collects personal information of users, take reasonable steps, to notify them of the following: • Its identity and contact details. • Any collections from third parties. • Where relevant, that a collection is required by law and the relevant law. • The purposes of collection. • The main consequences for the individual if all or some of the personal information is not collected. • Any other entity, body or person, or the types of any other entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected. • The privacy policy contains information about how the individual may access their personal information and seek the correction of such information. • The Privacy Policy contains information about how the individual may lodge a complaint. • Whether the entity is likely to disclose the personal information to overseas recipients (and if so, where).
3.6 Collection and use limitation	**2.6 Collection and use limitation**
TDIF Req: PRIV-03-06-01; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST only collect Personal information that it is permitted to collect under law and that is reasonably necessary for one or more of its functions or activities directly relating to identity verification.	The Applicant MUST ensure that: • It only collects personal information that is reasonably necessary for one or more of its functions or activities relating to identity verification.
TDIF Req: PRIV-03-06-02; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST only collect Personal information by lawful and fair means.	• It only collects information by lawful and fair means.

TDIF Req: PRIV-03-06-03; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST only collect Personal information from the Individual or their representative, unless it is unreasonable or impractical to do so.	• It only collects information from the individual or their representative, unless it is unreasonable or impractical to do so.
–	• It only collects sensitive information where it is required or authorised by or under an Australian law or court order or is otherwise authorised under APP 3.4.
–	• The individual has consented to his/her identity attributes being disclosed before he/she verifies to a Relying Party.
–	• Only discloses 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 is required).
TDIF Req: PRIV-03-06-04; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST NOT use Personal information for direct marketing purposes as defined in APP 7.	The Applicant MUST NOT use personal information for direct marketing purposes.
–	The Applicant MUST comply with APP 6 for all uses and disclosures as well as complying with more specific Privacy Requirements relating to consent (2.9), direct marketing (2.6), behavioural information (2.7) and biometric information (2.8)). [For example even if APP 6.2 allows the disclosure of identity attributes to a relying party because it is related to the primary purpose and within reasonable expectations, the Exchange must still obtain consent to pass those attributes due to the more specific requirements in the TDIF Privacy Requirements 2.9.]
TDIF Req: PRIV-03-06-05; Updated: Mar-20; Applicability: X The Applicant MUST publish in an open and accessible manner an Annual Transparency Report that discloses the scale, scope and reasons for access to Personal information (including metadata) by an enforcement body, as defined in the Privacy Act. **TDIF Req: PRIV-03-06-06;** Updated: Mar-20; Applicability: X The Applicant MUST NOT retain Users’ Attributes once they are passed from an Identity Service Provider to a Relying Party with the exception of securely storing the attributes for the duration of an authenticated session.	**2.6.1 Identity Exchange additional requirements** If the Applicant is an Identity Exchange, it: • MUST 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. • MUST NOT retain users’ attributes once they are passed from the Identity Service Provider to the Relying Party.

3.7 Limitation on use of behavioural information **TDIF Req: PRIV-03-07-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST only collect, use and disclose information about an Individual's behaviour on the Australian Government's identity federation to: a) Verify the Identity of an Individual and assist them to receive a digital service from a relying party. b) To support identity fraud management functions. c) To improve the performance or usability of the Applicant's identity system. d) To de-identify the data to create aggregate data.	**2.7 Limitation on use of behavioural information** An Applicant who collects personal information about an individual's behaviour (such as history and frequency of services received, credential preferences or Identity Service Provider preferences) MUST NOT use or disclose that information (for example to sell the data, target a person for compliance activities) except to: • Verify the person and assist them to obtain the service they are seeking, including assisting a relying party to offer the service. • Detect/identify/investigate/report fraud on the identity system. • Improve the product or service (ie understanding user pain points and system performance).
3.8 Collection and disclosure of biometrics **TDIF Req: PRIV-03-08-01;** Updated: Mar-20; Applicability: I The Applicant MUST only collect Sensitive information (including Biometric information) as outlined in APP 3.3 and 3.4. **TDIF Req: PRIV-03-08-02;** Updated: Mar-20; Applicability: I Biometric information collected to for the purpose of proofing an Individual's Identity MUST be destroyed once the Biometric information has been used to verify that identity (for example it has been matched against a source photograph), unless: • The Individual chooses to retain the Biometric information stored or controlled by the Individual on their device, or • The Biometric information is collected or was collected to create a government Identity document (for example where a Road Traffic and Transport Authority is a, Identity document issuer and an Identity Service Provider) **TDIF Req: PRIV-03-08-03;** Updated: Mar-20; Applicability: I Biometric information collected to prove an Individual's Identity MUST NOT be used and disclosed for purposes other than those listed in TDIF Req: PRIV-03-08-02.	**2.8 Collection and use of biometrics** 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 provide evidence of identity (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 other than a third party verifying the biometric. • MUST be destroyed once the verification process has concluded.

3.9 Consent **TDIF Req: PRIV-03-09-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST obtain Express Consent from an Individual prior to disclosing the individual's Attributes to a Relying Party or any third party. **TDIF Req: PRIV-03-09-01a;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST only disclose the Individual's Attributes required for the Relying Party's transaction with that Individual's Consent. **TDIF Req: PRIV-03-09-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST allow an Individual to withdraw their Consent. **TDIF Req: PRIV-03-09-02a;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate how this Consent withdrawal process is straightforward and easy to use. **TDIF Req: PRIV-03-09-02b;** Updated: Mar-20; Applicability: A, C, I, X An Individual MUST be made aware of the implications of providing or withdrawing their Consent. **TDIF Req: PRIV-03-09-03;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST maintain auditable logs that demonstrate that Consent was obtained and is current. **TDIF Req: PRIV-03-09-03a;** Updated: Mar-20; Applicability: A, C, I, X The auditable logs MUST NOT contain Biometric information. **TDIF Req: PRIV-03-09-04;** Updated: Mar-20; Applicability: A, I The Applicant MUST inform Individuals of other channels available to verify Identity and make clear to the User what the consequences are of declining to provide Consent or the required information.	**2.9 Consent** The exchange MUST obtain consent from an individual prior to it disclosing attributes to a Relying Party. Note: Valid consent includes: • The individual is adequately informed before giving consent. • Consent is voluntary. • Consent is current and specific. The individual has the capacity to understand and communicate their consent. An individual MAY withdraw their consent at any time, and the process to do this MUST be easy to use and straightforward. 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. The Applicant MUST maintain auditable logs that demonstrate that consent was obtained and is current.
TDIF Req: PRIV-03-09-05; Updated: Mar-20; Applicability: A, I The Applicant MUST obtain Consent to verify Identity Attributes against an Authoritative Source. For example, through an Identity Matching Service.	**2.9.1 Identity Service Provider additional requirements** If the Applicant is an Identity Service Provider it MUST: • Seek and obtain consent to verify identity attributes at the source such as through the Document Verification Service (DVS) and Face Verification Service (FVS). • Permanently close a user's account at the request of a user, even if some attributes are retained for some time.
3.10 Cross border and contractor disclosure of Personal information **TDIF Req: PRIV-03-10-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate how it complies with APP 8 – cross border disclosure of Personal information. **TDIF Req: PRIV-03-10-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST take reasonable steps to ensure an overseas recipient of Personal information used by the Applicant to provide its identity system only uses the Personal information disclosed to it for purposes directly related to identity verification. **TDIF Req: PRIV-03-10-02a;** Updated: Mar-20; Applicability: A, C, I, X If it discloses Personal information to an overseas recipient that is not the individual, the Applicant MUST demonstrate to the Oversight [Authority]s' reasonable satisfaction it has appropriate contractual and practical measures to ensure the overseas recipient complies with these TDIF privacy requirements.	**2.10 Cross border and contractor disclosure** Applicants MUST comply with APP 8 – cross border disclosure of personal information. In addition, before an Applicant discloses personal information to an overseas recipient as part of running the Applicant (for example an overseas cloud host), the Applicant MUST take such steps that are reasonable to ensure the recipient only uses the information for purposes related to identity verification. When the Applicant contracts the operation of a part of its business covered by the TDIF, the Applicant MUST provide evidence to the TDIF Accreditation Authority that it has appropriate contractual and practical measures to ensure the contractor is complying with these Privacy Requirements. See the *TDIF: Protective Security Requirements* for more information on security and contract management.
3.11 Government Identifiers **TDIF Req: PRIV-03-11-01;** Updated: Mar-20; Applicability: X The Applicant MUST NOT create a new government identifier for use across the identity federation (i.e., an identifier that is sent to more than one Relying Party or Identity Service Provider).	**2.11 Government Identifiers** Applicants that are organisations as defined by the Privacy Act MUST comply with their obligations under APP 9 which relate to the adoption, use and disclosure of government related identifiers.

	An Applicant MUST NOT create a new government identifier that is used across the identity federation (i.e., an identifier that is sent to more than one Relying Party or Identity Service Provider).
3.12 Access, correction and individual history log	**2.12 Access, correction and consumer history log**
3.12.1 Access **TDIF Req: PRIV-03-12-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST on request by an Individual, give that Individual access to the Personal information it holds about the Individual, unless an exception is available under APP 12 (APP 12.2 for Commonwealth agencies and APP 12.3 for other Applicants). **TDIF Req: PRIV-03-12-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST respond to a request for access to Personal information that it holds from an individual within 30 days after the request is received. **TDIF Req: PRIV-03-12-03;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST give the Individual access to their Personal information in the manner requested by the Individual, if it is reasonable, secure and practicable to do so. **TDIF Req: PRIV-03-12-04**; Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST provide access at no cost to the Individual. **TDIF Req: PRIV-03-12-05;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST where access is refused, take steps to meet the needs of the Individual and provide a written notice as set out in APP 12.	**2.12.1 Access** The Applicant MUST: • Where it holds personal information about an individual, on request by the individual, give the individual access to the information. o Unless an exception is available under APP 12 (APP 12.2 for Commonwealth agencies and APP 12.3 for other Applicants). • Respond to the request for access to personal information within 30 days after the request is made. • Give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so. • Provide access for free. • Where access is refused, take steps to meet the needs of the individual and provide a written notice as set out in APP 12.
3.12.2 Correction **TDIF Req: PRIV-03-12-06;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST allow Individuals to correct their Personal information it holds as set out in APP 13. **TDIF Req: PRIV-03-12-07;** Updated: Mar-20; Applicability: A, C, I The Applicant MUST provide Individuals with a simple and accessible means to access and review their Personal information. **TDIF Req: PRIV-03-12-07a;** Updated: Mar-20; Applicability: A, C, I The Applicant MUST provide Individuals with a channel to update their Personal information in near to real time.	**2.12.2 Correction** The Applicant MUST: • Allow individuals to correct their personal information as set out in APP 13. • Provide individuals with a simple means to review and update their personal information on an ongoing basis.
3.12.3 Individual history log **TDIF Req: PRIV-03-12-08;** Updated: Mar-20; Applicability: X The Applicant MUST provide Individuals with a centralised view of the metadata of services the Individual accessed, the time of access and the Attributes passed to the Relying Party unless such information has already been destroyed by the Applicant in accordance with the TDIF.	**2.12.3 Consumer history log** If the Applicant is an Identity Exchange it MUST provide individuals with access to the metadata on transactions it logs (i.e., that has not been deleted under its destruction policy) in one place. The log SHOULD include the services the individual accessed, the time of access and the attributes passed to the service. 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.

3.13 Quality of personal information **TDIF Req: PRIV-03-13-01;** Updated: Mar-20; Applicability: A, C, I, X An Applicant MUST take reasonable steps to ensure quality of Personal information as outlined in APP 10. **TDIF Req: PRIV-03-13-02**; Updated: Mar-20; Applicability: A, C, I The Applicant MUST implement internal practices, procedures and systems (including training Personnel in these practices, procedures and systems) to audit, monitor, identify and correct poor-quality Personal information. **TDIF Req: PRIV-03-13-03;** Updated: Mar-20; Applicability: A, C, I The Applicant MUST ensure updated or new Personal information is promptly added to relevant existing records.	**2.13 Quality of personal information** The Applicant MUST: • Take reasonable steps to ensure that the personal information it collects is, having regard to the purpose of the use or disclosure is accurate, up-to-date, complete, relevant and not misleading. • Take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure is accurate, up-to-date, complete, relevant and not misleading. **2.13.1 Identity Service Provider additional requirements** If the Applicant is an Identity Service Provider it MUST: • Implement internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems). • Ensure updated or new personal information is promptly added to relevant existing records. • Provide individuals with a simple means to review and update their personal information on an ongoing basis.
3.14 Handling Privacy Complaints **TDIF Req: PRIV-03-14-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST provide a complaints service for handling privacy complaints which: a) is readily accessible, including prominent contact information about the service. b) is fair, including a process that is impartial, confidential and transparent. c) has a process that is timely, clear and can provide a remedy where applicable. d) has skilled and professional people who have knowledge of privacy laws and these TDIF privacy requirements and the complaint service process. e) is integrated with other complaint handling bodies, (e.g., other Participants of an identity federation) as required, so it can assist the individual and refer complaints.	**2.14 Handling Privacy Complaints** The Applicant MUST provide a complaints service which: • Is accessible, including prominent contact information about the service. • Is fair, including a process that is impartial, confidential and transparent. • Has a process which is timely, clear and can provide a remedy. • Has skilled and professional people who have knowledge of privacy laws and these Privacy Requirements and the complaint service process. • Is integrated with other complaint handling bodies, (e.g., other participants of the identity federation) so it can assist the user and refer complaints. • Analyses complaint information, including complaint processes, and feeds conclusions into privacy risk planning and improving documentation and processes. • Publishes de-identified information and analysis about complaints. The Applicant MUST participate in a service that enables agreed de-identified data on complaints to be shared across participants in the identity federation to ensure participants learn from complaints.

3.15 Destruction and de-identification **TDIF Req: PRIV-03-15-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate it takes reasonable steps to destroy or de-identify Personal information in line with APP 11.2.	**2.15 Destruction and de-identification** The Applicant MUST ensure that: • It takes reasonable steps to destroy or de-identify personal information once it is no longer needed for identity verification and related administrative purposes, unless retention is required under law. • It has a written management policy that specifies: o Whether stored personal information needs to be retained under law or a court/tribunal order. o Data retention timeframes. o De-identification policies and practices (including mitigation of the risk of re identification). o Data destruction policies and practices. • All staff are informed of document destruction and de-identification procedures. • Where required, personal information contained in hard copy records is destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding. • Hardware containing personal information (including back-ups) in electronic form is 'sanitised' in accordance with Australian Signals Directorate requirements to completely remove the stored personal information. • Where personal information is stored on a third-party's hardware (e.g., cloud storage) procedures are in place to verify that instructions to irretrievably destroy/de-identify the personal information have been complied with.
7 Functional Assessments The Applicant is required to undergo a series of Functional Assessments by Assessors. These Functional Assessments include: • A Privacy Impact Assessment. • A Privacy assessment. • A Security assessment. • A Penetration test. • A Web Content Accessibility Guidelines (WCAG) assessment.	

7.1 PIA and Privacy Assessment **TDIF Req: ASSESS-07-01-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST commission an Assessor to conduct a Privacy Impact Assessment on their identity system as part of accreditation. **TDIF Req: ASSESS-07-01-02;** Updated: Mar-20; Applicability: A, C, I, X Once accredited, the Applicant MUST conduct a Privacy Impact Assessment on all high-risk projects related to their identity system. **TDIF Req: ASSESS-07-01-03;** Updated: Mar-20; Applicability: A, C, I, X The Privacy Impact Assessment conducted MUST: a) Be undertaken early enough to influence the design of the identity system. b) Reflect consultation with relevant stakeholders. c) Include a description of the proposed identity system. d) Map the identity system's personal information flows. e) Include an analysis of risks of non-compliance with relevant privacy laws and TDIF privacy requirements. f) Include an analysis of the impact of the project on the privacy of Individuals. g) Include an analysis of whether privacy impacts are necessary or avoidable. h) Include an analysis of possible mitigations to privacy risks. i) Include recommendations	**2.3 Privacy Impact Assessment** As part of the TDIF Accreditation Process, the Applicant: • MUST commission a PIA, by a Privacy Impact Assessor to review the privacy impacts of the Applicant's identity service. o A Privacy Impact Assessor is a separate legal entity to the Applicant, not under the Applicant's control and has knowledge and experience in conducting PIAs. • MUST conduct a PIA for all high privacy risk projects related to its identity service. o A project may be a high privacy risk project if the Applicant reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals. • SHOULD publish the above mentioned PIAs, or a summary version or an edited copy of the PIA, on its website. • MUST respond in writing, at a senior management level, to the recommendations outlined in the PIA including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations. • MUST maintain a register of the PIAs it conducts and response. • MUST publish the register, or a version of the register, on its website. A PIA SHOULD be conducted using the [OAIC] Guide to undertaking privacy impact assessments. A PIA MUST at a minimum: • Be conducted by a Privacy Impact Assessor • Be in writing. • Be conducted early enough to influence the design of a project or decision. • Reflect consultation with relevant stakeholders. • Include a description of the proposed project. • Map the project's information flows. • Include an analysis of: o Risks of non-compliance with the relevant laws related to privacy. o Risks of non-compliance with these Privacy Requirements. o The impact of the project on individuals. o Whether privacy impacts are necessary or avoidable. o Possible mitigation of risks. • Provide recommendations to the TDIF Accreditation Authority.

7.4 Applicant obligations **TDIF Req: ASSESS-07-04-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST undergo each Functional Assessment. **TDIF Req: ASSESS-07-04-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST define the scope, objectives and criteria for each Functional Assessment and provide this to the DTA as part of its Accreditation Plan. **7.5 Assessor skills, experience and independence** **TDIF Req: ASSESS-07-05-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate to the DTA how the Assessors have relevant, reasonable and adequate experience, training and qualifications to conduct the Functional Assessment. **TDIF Req: ASSESS-07-05-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST demonstrate to the DTA how the Assessors: • Are independent from the development and operational teams of the Applicant's identity system. • Do not possess a conflict of interest in performing the Functional Assessment on the Applicant's identity system.	
7.6 Assessment process **TDIF Req: ASSESS-07-06-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST ensure Assessors have access to and consider all relevant evidence provided by the Applicant to the DTA. This includes any responses by the DTA to questions which may have been asked. **TDIF Req: ASSESS-07-06-02;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST ensure Assessors conduct the Functional Assessments. **TDIF Req: ASSESS-07-06-03;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST use the compliance ratings listed in 'Appendix A: Compliance ratings' when determining areas of compliance and non-compliance with the requirements of the TDIF. **TDIF Req: ASSESS-07-06-04;** Updated: Mar-20; Applicability: A, C, I, X The Functional Assessments MUST include: a) Documentation reviews. b) Interviews with key personnel. c) A run through of the Applicant's identity system. **TDIF Req: ASSESS-07-06-05;** Updated: Mar-20; Applicability: A, C, I, X The Functional Assessment MAY include a site visit to the Applicant's premises or other location where it provides services in connection with its identity system.	
7.7 Functional Assessment Report **TDIF Req: ASSESS-07-07-01;** Updated: Mar-20; Applicability: A, C, I, X The Applicant MUST ensure the Assessors document the outcomes of the assessment in a Functional Assessment Report. **TDIF Req: ASSESS-07-07-01a;** Updated: Mar-20; Applicability: A, C, I, X The Applicant's Accountable Authority MUST respond in writing, to the recommendations outlined in the Functional Assessment Report including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations.	

TDIF Req: ASSESS-07-01-04; Updated: Mar-20; Applicability: A, C, I, X The Applicant's identity system MUST undergo a Privacy Assessment (which is separate to and follows on from the PIA) as part of initial accreditation and annually thereafter as part of the Annual Assessment. [Galexia Note: Annual Assessment extracted below]	
TDIF Release4, 07 Annual Assessments (March 2020, version 1.0)	
TDIF Release 4, 07 – Annual Assessment [Galexia Note: Following extracts relevant to privacy] **2 Maintain TDIF accreditation** To maintain TDIF accreditation, the Accredited Participant is required to undergo an Annual Assessment by suitably skilled and experienced Assessors. **2.2 Accredited Participant obligations** **TDIF Req: ANNUAL-02-02-01;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant MUST ensure that all Annual Assessment requirements are completed by the anniversary of its initial accreditation date. Failure by an Accredited Participant to complete the Annual Assessment in accordance with the TDIF is a breach of the Accredited Participant's obligations under the TDIF and may result in the termination of accreditation. **2.3 Assessor skills, experience and independence** **TDIF Req: ANNUAL-02-03-01;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant MUST demonstrate to the DTA how the Assessors have relevant, reasonable and adequate experience, training and qualifications to conduct the Annual Assessment. **TDIF Req: ANNUAL-02-03-01a;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant MUST demonstrate to the DTA how the Assessors: • Are independent from the development and operational teams of the Accredited Provider's identity system. • Do not possess a conflict of interest in performing the Annual Assessment on the Accredited Participant's identity system. **2.4 Annual Assessment schedule** **TDIF Req: ANNUAL-02-04-01;** Updated: Mar-20; Applicability: A, C, I, X Annual Assessments that occur during: • Even calendar years (i.e., 2020, 2022, 2024, etc) MUST be undertaken by Assessors who are external to the Accredited Participant's organisation. • Odd calendar years (i.e., 2021, 2023, 2025, etc) MAY be undertaken by Assessors who are external to the development and operational teams of the Accredited Provider's identity system. **2.4.1 Annual Assessment process** **TDIF Req: ANNUAL-02-04-02;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant MUST ensure Assessors have access to and consider all relevant evidence provided by the Accredited Participant to the DTA. This includes any responses by the DTA to questions which may have been asked. **TDIF Req: ANNUAL-02-04-03;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant MUST ensure Assessors conduct the Annual Assessments and prepares the Annual Assessment Report in accordance with the requirements of the TDIF.	**3 Part two: privacy audit** **3.1 Purpose and context of the privacy audit** This section outlines the requirements and provides some guidance for Applicants and Privacy Assessors when conducting the privacy audit as part of the TDIF Accreditation Process. • Determine whether the Applicant can demonstrate it has complied with these Privacy Requirements. • Determine whether the Applicant has addressed all recommendations arising from the PIA. • Document the results of the privacy audit in a report to the TDIF Accreditation Authority. The following activities have occurred by the time the privacy audit is undertaken: • The Applicant has provided the TDIF Accreditation Authority with a plan demonstrating how they will meet these Privacy Requirements. • The Applicant has provided the TDIF Accreditation Authority with privacy documentation including a Privacy Management Plan and Data Breach Plan. The full list of privacy documentation is outlined above in the 'Privacy Requirements' section of this document. • An independent body has conducted a PIA on the Applicant. • The Applicant has provided the TDIF Accreditation Authority with a report which outlines how and by when they will address the recommendations outlined in the PIA. • As part of the TDIF Accreditation Process the Applicant has submitted protective security, risk management and fraud control documentation to the TDIF Accreditation Authority. This provides additional context to the privacy audit. **3.2 Privacy audit process** The Privacy Assessor MUST carry out the following steps as part of the privacy audit: • Evaluate assessments or comments already made by the TDIF Accreditation Authority. • Evaluate all relevant evidence provided by the Applicant to the TDIF Accreditation Authority. This includes any responses to questions which may have been asked. • Once the documentation has been reviewed, define the scope, objectives and criteria of the privacy audit as part of an audit plan. • Conduct the privacy audit. At a minimum this MUST include: o Documentation reviews. o Conduct a site visit. o Interview key privacy and operations personnel. • The Privacy Assessor MUST retain evidence to support its findings. The Privacy Assessor will only need to provide evidence indicated in the privacy audit tool below to the TDIF Accreditation Authority as part of its report. • Provide the Applicant with reasonable opportunity to provide feedback on its evidence and findings. • Provide the Applicant with reasonable opportunity to respond to the report's findings, including the actions and timeframes in which remediation actions will occur. This is required if non-compliance issues are identified.

TDIF Req: ANNUAL-02-04-04; Updated: Mar-20; Applicability: A, C, I, X
The Accredited Participant MUST use the compliance ratings listed in 'Appendix A: Compliance ratings' when determining areas of compliance and non-compliance with the requirements of the TDIF.

TDIF Req: ANNUAL-02-04-05; Updated: Mar-20; Applicability: A, C, I, X
The Annual Assessments MUST include:

a) Documentation reviews.

b) Interviews with key personnel.

c) A run through of the Accredited Participant's identity system.

TDIF Req: ANNUAL-02-04-05a; Updated: Mar-20; Applicability: A, C, I, X
The Annual Assessment MAY include a site visit to the Accredited Participant's premises or other location where it provides services in connection with its identity system.

TDIF Req: ANNUAL-02-04-06; Updated: Mar-20; Applicability: A, C, I, X
As part of the Annual Assessment the Accredited Participant MUST provide the DTA with:

a) One or more Annual Assessment Reports in accordance with the requirements set out in the following sections of this document.

b) An annual Qualifying Attestation Letter in accordance with the requirements set out in the following sections of this document.

Upon receipt of the Annual Assessment Report and Qualifying Attestation Letter, the DTA will conduct a review of the documents and advise the Accredited Participant of its acceptance of the documents and whether or not they meet TDIF requirements. This includes whether the proposed remediation actions, and timings, are acceptable. The Accredited Participant MUST remediate any non-compliances or adverse findings to the satisfaction of the DTA within agreed timeframes. The outcome of the Annual Assessment is an Annual Assessment Report and a Qualifying Attestation Letter. The Annual Assessment Report details the Accredited Provider's identity system compliance against TDIF requirements. This includes areas of compliance and non-compliance against the TDIF and any suggested remediation actions.

2.5 Annual Assessment reporting

TDIF Req: ANNUAL-02-05-01; Updated: Mar-20; Applicability: A, C, I, X
The Accredited Participant MUST ensure that the Assessor prepares Annual Assessment Reports which cover:

a) The Privacy Assessment (as per ASSESS-06-02-04).

b) The security assessment (as per ASSESS-06-03-01).

c) The penetration test (as per ASSESS-06-03-02).

d) An annual usability test (as per UX-05-05-02)

e) An assessment against at least version 2.0 of the Web Content Accessibility Guidelines (WCAG) (as per ASSESS-06-04-01).

TDIF Req: ANNUAL-02-05-02; Updated: Mar-20; Applicability: A, C, I, X
As part of the Annual Assessment the Accredited Participant MUST provide the DTA with:

a) Any decisions and supporting documentation made by the Accredited Participant's Accountable Authority to vary its fraud control arrangements during the year (as per FRAUD-02-01-03).

b) Evidence of the Accredited Participant's Fraud Control Plan (and supporting Fraud Control Plans) being reviewed during the year (as per FRAUD-02-02-02).

c) A copy of fraud awareness training materials provided by the Accredited Participant to Personnel during the year (as per FRAUD-02-03-01).

• Provide a report of findings (see Annex A: privacy audit template below) to the Authority. The report MUST at a minimum:

o Summarise the activities performed during the privacy audit.

o Advising whether or not the Applicant has complied with these Privacy Requirements, including any requirements that could not be adequately assessed due to access or timing issues.

o Recommends remediation actions to address any areas of non-compliance. o Include the Applicant's response to the privacy audit findings and recommendations.

3.3 Type of audit and auditor skills

The privacy audit is to determine whether the Applicant is compliant with these Privacy Requirements and has addressed the PIA recommendations. The Privacy Assessor MUST NOT take a 'tick box' approach to the requirements.

The privacy audit MUST be undertaken by a Privacy Assessor who is independent from the development team. Privacy Assessors can either be internal staff or third parties.

The Privacy Assessor MUST have relevant and adequate experience and training to carry out the privacy audit.

3.4 Privacy audit roles and responsibilities

3.4.1 TDIF Accreditation Authority

The TDIF Accreditation Authority is responsible for:

• Ensuring that the accreditation process is conducted with due care and in accordance with the published TDIF documents.

• Reviewing, within agreed timeframes, all relevant Applicant documentation to ensure conformance to the published TDIF documents.

• Providing relevant documentation, it holds on an Applicant to the auditor.
• Considering all reports and recommendations from Privacy Assessors.
• Notify the Applicant of any non-compliance issues, required mitigation actions and timeframes for the mitigations.

• All decisions in relation to the suitability of an Applicant to be accredited.

3.4.2 The Applicant

The Applicant is responsible for:

• Obtaining the services of an auditor.

• Preparing and providing all information requested by the auditor.

• Supporting the auditor as required during the privacy audit.

3.4.3 Privacy Assessor

The Privacy Assessor is responsible for:

• Assessing the Applicant's compliance against these Privacy Requirements. • Documenting their findings, which:

o Summarise the activities performed during the evaluation.

o Suggest remediation actions to address areas of non-compliance or unmitigated risk.

o Recommend whether or not the Applicant has satisfied these Privacy Requirements.

• Providing their findings to the TDIF Accreditation Authority.

d) Evidence of the Accredited Participant's Privacy Policy being reviewed and where relevant updated during the year (as per PRIV-03-02-05). e) Evidence of the Accredited Participant's Privacy Management Plan being reviewed and where relevant updated during the year (as per PRIV-03-02-07) f) A copy of privacy awareness training materials provided by the Accredited Participant to Personnel during the year (as per PRIV-03-02-08). g) For Identity Exchanges, a copy of their Annual Transparency Report (as per PRIV-03-06-05). h) Any decisions and supporting documentation made by the Accredited Participant's Accountable Authority to vary its protective security control arrangements during the year (as per PROT-04-01-03). i) A copy of protective security training materials provided by the Accredited Participant to Personnel during the year (as per PROT-04-01-07). j) Evidence of the Accredited Participant's System Security Plan (and supporting System Security Plans) being reviewed during the year (as per PROT-04-01-13). k) Any decisions and supporting documentation made during the year by the Accredited Participant's Chief Security Officer (or their delegate) to implement alternative mitigation measures or controls to those listed in the TDIF: 04 – Functional Requirements (as per PROT-04-01-18). l) Evidence that the Accredited Participant's Disaster Recovery and Business Continuity Plan has been tested during the year (as per PROT-04-02-27). m) Outcomes of its annual usability test conducted on its identity system (as per UX-05-05-04a). n) For Identity Service Providers, processes and risk assessments to support exception cases (as per IDP-03-03-01b) o) For Attribute Service Providers, evidence of its arrangements with an Authoritative Source (as per ASP-05-02-01a) p) Evidence that the Accredited Participant has reviewed the conditions under which a TDIF Exemption Request has been granted (As set out in B.2.5 of the TDIF: 03 Accreditation Process). q) The evaluation, results and report for the presentation attack detection technology used by the Accredited Participant (as per IDP-03-09-10b as set out in Appendix B of the TDIF: 05 – Role Requirements). r) A copy of Manual Face Comparison training materials provided by the Accredited Participant to Personnel during the year (as per IDP-03-09-23 as set out in Appendix B of the TDIF: 05 – Role Requirements). **TDIF Req: ANNUAL-02-05-03;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant's Accountable Authority MUST respond in writing to the recommendations outlined in the Annual Assessment Report including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations. **TDIF Req: ANNUAL-02-05-04;** Updated: Mar-20; Applicability: A, C, I, X The Annual Assessment Reports MUST include the following: a) The date of and period covered by the report. b) Name, role (or position) and contact details of the relevant Accountable Authority and point of contact within the Accredited Participant's organisation. c) Qualifications and basis of independence for all Assessors used. d) Names and version numbers of all documents used by the Accredited Participant. e) City, state and (if applicable) country of all physical locations used in the Accredited Participant's operations. This includes data centre locations (primary and alternative sites) and all other locations where general ICT and business process controls that are relevant to the Accredited Participant's operations are performed.	

f) The test or evaluation methodology(s) used. g) The test or evaluation results. h) Findings. i) Remediation actions or recommendations to address any areas of non-compliance. j) Express an opinion and provide recommendations to the DTA of the Accredited Participant's identity system against the TDIF requirements, including any requirements that could not be adequately assessed due to access or timing issues. k) Include a list of compliant and non-compliant controls. l) Where a non-compliance has been identified, the remedial actions and timeframes within which actions will be completed to address the non-compliance. **TDIF Req: ANNUAL-02-05-05;** Updated: Mar-20; Applicability: A, C, I, X The Accredited Participant MUST: • Provide a copy of the full findings and report to the DTA, or • Enable the DTA access to a copy of the findings and report. An executive summary or redacted version of the findings or report is insufficient to meet this requirement.	

Appendix 3 – PIA3 Recommendation Summary and DTA response

Galexia Note: The Recommendation Summary and DTA's response has been moved to Section 2. PIA3 Recommendation Summary and DTA response (October 2021).

Appendix 4 – Initial and Second PIA Recommendation Summary

Prior PIAs have 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 the PIAs and includes *previous* recommendations made in PIA1 and PIA2, many of which have been implemented:

PIA1 (December 2016) Recommendations

Component / APP	Recommendation	Action Required	Person / Agency responsible
Component 1. Mandatory policies and standards	**Recommendation 1: The TDIF accreditation / revocation proposal** The development of the TDIF membership proposal, including accreditation and revocation, would benefit from significant further work on developing the detailed provisions and legal backing / powers / national agreement for the proposal, followed by further consultation with stakeholders. Stakeholders currently have very low expectations that this aspect of the TDIF can be developed or enforced.	**2016 Action:** Clarify and explain the detailed powers behind this proposal	DTA
	Recommendation 2: Privacy principles in the Core Service Requirements The DTA should consider the full range of options for incorporating privacy principles in the TDIF Core Service Requirements). The strengths and limitations of each option should be considered side by side, and discussed with key stakeholders. This discussion would benefit from the development of draft principles that attempt to set the highest possible standard based on existing laws in each jurisdiction, but this option should not be the only option available for discussion. Practical issues for the implementation of each option should also be considered, and solutions proposed.	**2016 Action:** Develop a set of draft Privacy Principles and consult with stakeholders	DTA
Component 2. The Identity Exchange	**Recommendation 3: The Identity Exchange and the retention of metadata** DTA should conduct further research on the period that meta-data needs to be retained in order to facilitate the investigation of identity fraud and suspicious transactions. This period should then be 'balanced' against the privacy risks and impacts of retaining the data, and an appropriate data retention period should be incorporated into the design of the Identity Exchange. For the avoidance of doubt, an 'appropriate period' could be shorter than the period required for all investigative purposes.	**2016 Action:** Determine a specific meta-data retention period	DTA
Component 3. Identity Providers (IdPs)	**Recommendation 4: The selection of a single Commonwealth IdP – further consultation** The DTA should recognise stakeholder concerns regarding the decision to establish a single Commonwealth IdP and should take steps to ensure that the proposal has an appropriate level of stakeholder and community understanding and support before implementing the proposal.	**2016 Action:** Further stakeholder engagement (workshop / consultation)	DTA
	Recommendation 5: The selection of a single Commonwealth IdP – risk assessment The DTA should commission an independent risk assessment of the proposal to establish a single Commonwealth IdP, in comparison to the risks of other options, to ensure that the consequences of the proposed model do not represent an unacceptable risk to the community.	**2016 Action:** Completion of a detailed risk assessment	Independent provider
Is the data 'personal information' ?	**Recommendation 6: Identity Providers and the definition of Personal Information** All data collected, stored and used by Identity Providers (IdPs) should be classified and treated as Personal Information.	**2016 Action:** The TDIF Core Service Requirements should classify all data used by Identity Providers (IdPs) as Personal Information.	DTA

	Recommendation 7: The Identity Exchange and the definition of Personal Information All data collected, stored and used by the Identity Exchange should be classified and treated as Personal Information.	**2016 Action:** The Identity Exchange documentation should classify all data as personal information.	DTA
APP 1: Open and Transparent Management of Personal Information	**Recommendation 8: Openness Task** Specific requirements on openness and transparency should be set out in the TDIF Core Service Requirements. – IdPs will be required to develop a stand-alone privacy policy and submit it as part of their TDIF application. – Relying Parties will need to amend or expand their existing privacy policies to incorporate references to key data collection, use and disclosure that is facilitated by the TDIF. – The Identity Exchange will need to develop a stand- alone privacy policy.	**2016 Action:** The Identity Exchange should develop a specific privacy policy	DTA
APP 3: Collection of solicited personal information	**Recommendation 9: Collection of sensitive data** The next iteration of the TDIF design will need to incorporate a request for specific explicit consent from users to the collection of biometric data. This occurs at the enrolment stage. The project would benefit from some further user testing regarding whether users understand the consent that they are providing in relation to the collection of biometric data.	**2016 Action:** 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
APP 5: Notification	**Recommendation 10: Notice requirements** Notice will need to be provided by: – IdPs – at the time they enrol individuals and again when individual log in to the service to manage their identities or make an inquiry; – Relying Parties – at the time they refer consumers to the Identity Exchange; and – The Identity Exchange – at the time consumers visit the Exchange to select an IdP for enrolment, and again at the time they visit the Exchange to select an IdP for authentication.	**2016 Action:** 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
APP 6: Use or Disclosure	**Recommendation 11: Secondary use for investigating identity fraud and suspicious transactions** The exact scope and rules for the investigation of identity fraud and suspicious transactions by TDIF participants should be addressed in the TDIF Core Service Requirements and other TDIF documentation. The extent of this secondary use should be disclosed to consumers.	**2016 Action:** 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
	Recommendation 12: Use of biometric data APP 6 provides some additional rules for the use and disclosure of biometric data. However, the detailed provisions are delegated to 'guidelines' which have not yet been developed. In the meantime, the TDIF Core Service requirements should incorporate some additional privacy protections for the use of biometric data in the TDIF. These should include (at least): **A)** A strict prohibition on the biometric data being used for any secondary purpose (i.e., it would be restricted to verification of a photograph during initial enrolment); **B)** A requirement for all biometric data to be destroyed once the photograph has been verified; and **C)** The extension of these rules to all TDIF participants (APP 6.3 only applies to government agencies).	**2016 Action:** The TDIF Core Service Requirements should incorporate some additional privacy protections for the use of biometric data.	DTA

	Recommendation 13: Development of a transparency report APP 6 requires entities to keep a written note of third-party access to data by law enforcement agencies. This is an area where the TDIF Core Service Requirements could help to strengthen privacy protections, beyond the very limited requirements in the Privacy Act. Emerging best practice is for organisations to issue annual 'transparency reports' that disclose the broad scale and scope of access requests by law enforcement agencies. The TDIF should adopt this approach and publish a regular transparency report.	**2016 Action:** The TDIF should publish an annual transparency report on law enforcement access.	DTA
APP 7: Direct Marketing	**Recommendation 14: Direct marketing prohibition** The use of TDIF personal data for direct marketing should be prohibited in the TDIF Core Service Requirements.	**2016 Action:** The use of TDIF personal data for direct marketing should be prohibited in the TDIF Core Service Requirements	DTA
APP 8: Cross Border Disclosure	**Recommendation 15: Cross border data transfer – mapping** Each TDIF participant should identify and map their cross-border data transfers. This is an important step in meeting the (expected) notice and protection provisions in the TDIF Core Service Requirements	**2016 Action:** Each TDIF participant should identify and map their cross-border data transfers.	DTA / IdPs
	Recommendation 16: Cross border data transfer – protection Cross border data transfers in the TDIF should be permitted subject to the development of a single, consistent mechanism for protecting privacy in such transfers. The protection mechanism should be included in the TDIF Core Service Requirements. For the avoidance of doubt the protection mechanism could be both stronger and less flexible than the approaches permitted in current privacy law (particularly APP 8 in the Commonwealth Privacy Act), in order to meet the objective of consistent privacy protection throughout the TDIF.	**2016 Action:** The TDIF Core Service Requirements should include stronger and more consistent principles on cross border disclosures.	DTA
APP 9: Government Related Identifiers	**Recommendation 17: Restriction on the use of IdP identifiers** Unique identifiers developed by IdPs should not be adopted by any third party as their identifier and the disclosure of IdP identifiers should be severely restricted to specific situations requiring verification of identity.	**2016 Action:** 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
	Recommendation 18: Additional restriction on IdP identifiers In order to prevent function creep and scope creep (as far as possible) in relation to the use of IDP identifiers, the TDIF should adopt measures to ensure that identifiers in the TDIF are not to be used for purposes outside the TDIF. In addition, measures should be implemented to ensure that consumers will always have a choice of more than one IdP in any TDIF transaction.	**2016 Action:** Additional restrictions and guarantees should be implemented to prevent function creep and scope creep in relation to IdP identifiers.	DTA
APP 10: Quality of Personal Information	**Recommendation 19: Access requests – application in the TDIF** The TDIF Core Service Requirements should ensure that the Identity Exchange will provide access to the metadata on recent transactions, in order to assist consumers recognise suspicious transactions or identity fraud. In addition, each IdP will need to offer access to all the records that it holds on an individual, without restriction.	**2016 Action:** Each IdP will need to offer access to all the records that it holds on an individual, without restriction.	DTA / IdPs
	Recommendation 20: Access requests – consistency In the Commonwealth Privacy Act the requirement that access will be provided within 30 days only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants (including the private sector) to ensure a consistent experience for consumers. Similarly, the 'free access' requirement only applies to agencies, but in the TDIF it should be adopted as a common requirement across all TDIF participants.	**2016 Action:** The TDIF Core Service Requirements should adopt common access requirements across all IdPs.	DTA

APP 13: Correction	**Recommendation 21: Complaints coordination** It will be important to make the complaints and correction process 'clear and straightforward' for consumers. This may require TDIF participants to develop an appropriate referrals service. In addition, some data on complaints should be shared across the TDIF to ensure participants learn from complaints.	**2016 Action:** 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
	Recommendation 22: Complaints – Consistency In order to ensure a consistent experience for consumers, all TDIF participants should be required to respond to complaints within 30 days.	**2016 Action:** In order to ensure a consistent experience for consumers, all TDIF Participants should be required to respond to complaints within 30 days	DTA
Governance	**Recommendation 23: Governance arrangements** The DTA has recently commissioned a report on governance arrangements for the TDIF. The report should consider the following key governance issues (that have a direct impact on privacy protection): **A)** Ensuring complete structural separation between the Identity Exchange and IdPs; **B)** Ensuring an independent process is in place for TDIF accreditation; **C)** Developing an appropriate underlying legal authority for the TDIF; **D)** Developing appropriate coordination mechanisms for access and correction requests amongst TDIF participants, including the ability to share complaints data; and **E)** Developing an appropriate mechanism for TDIF membership and ongoing engagement with stakeholders.	**2016 Action:** 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

PIA2 (September 2018) Recommendations and DTA Response

Component / APP	Recommendation	DTA Response	Person / Agency responsible
Component 1. Mandatory policies and standards	**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.	**DTA Response (2018) – Agree – the Requirements should be strengthened:** 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.	DTA
Component 2. The Identity Exchange	**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.	**DTA Response (2018) – Need to explore further:** 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 (i.e., 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.	DTA / Identity Exchange
APP 1: Open and Transparent Management of Personal Information	**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.	**DTA Response (2018) – Agree:** We will make this a requirement in the next iteration of the privacy requirements	DTA / Participants
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** 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.	**DTA Response (2018) – Agree:** 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.	DTA
APP 10: Quality of Personal Information	**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.	**DTA Response (2018) – Agree:** We will include a time period for the validity and renewal of identity credentials in near term iteration of the proofing requirements	DTA

APP 13: Correction	**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	**DTA Response (2018) – Agree**	DTA
Governance	**Recommendation 30: Consumer and community representation in oversight of the TDIF** Key stakeholder representatives (from government, community and bus) 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**.**	**DTA Response (2018) – Agree:** 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.	DTA
	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.	**DTA Response (2018) – Agree:** We agree to a review three years after our first public beta service.	DTA

Appendix 5 – The Digital Identity System Background (as of July 2020)

The Digital Identity System

The following background summary was current as of July 2020 and was circulated as a background to stakeholders.

The Australian Government Digital Identity system is being developed by the Digital Transformation Agency (DTA) <www.dta.gov.au/our-projects/digital-identity>.

The Digital Identity system includes everything from the policy and processes to the technology and systems.

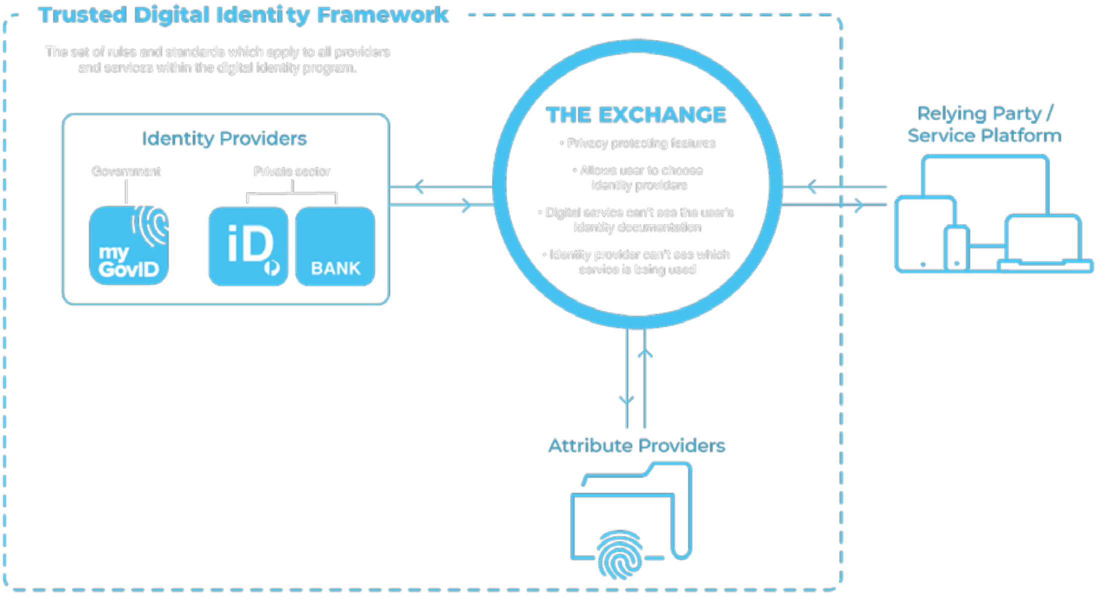
The DTA have summarised their vision for the future of digital identity in the following quote:

> *People are at the centre of everything the DTA does. The Australian Government is delivering the Digital Identity system, a program that will allow more government services to be available to people and businesses online at any time. Our vision is to provide simple, clear and fast public services through the use of a digital identity which will make access to government services more accessible and easier in a single, consistent way.*

The Digital Identity System is comprised of five main components:

1) The Exchange.
2) Identity Providers.
3) Attribute Providers.
4) Credential Service Providers.
5) Relying Parties.

This federation of different entities, all with their own role, is described in the following diagram:


Trusted Digital Identity Framework
The set of rules and standards which apply to all providers and services within the digital identity program.
Identity Providers
Government
Private sector
my GovID
iD
BANK
THE EXCHANGE
• Privacy protecting features
• Allows user to choose identity providers
• Digital service can't see the user's identity documentation
• Identity provider can't see which service is being used
Relying Party / Service Platform
Attribute Providers

- **The Exchange** mediates interactions between Identity Providers, Attribute Providers and Relying Parties. It enables the use of multiple Identity Service Providers through a single point of integration. The Exchange also protects the privacy of users through what is known as a 'double blind' and by transparently obtaining consent prior to passing attributes to relying parties. This means that an Identity Provider cannot see the service a user is accessing, and a Relying Party cannot see where a user has proved their identity. Essentially, neither party can identify the other during an interaction, helping to protect the user's privacy.

- **Identity Providers** allow users to create a Digital Identity and manage their Digital Identity once they have set it up. They bind verified identity information to credentials to create the Digital Identity. They verify an individual's personal information by checking the details on identity documents that a user voluntarily provides against government repositories of that information.
- **Attribute Providers** manage attributes relating to individual people and other entities, such as businesses. They verify special attributes relating to an individual's qualifications, entitlements and authorisations which can then be provided to Relying Parties via an Identity Exchange with the user's consent.
- **Credential Service Providers** generate, bind and distribute Credentials to individuals or can include the binding and management of credentials generated by individuals. This function may also be undertaken by an Identity Provider. A Credential is the technology used to authenticate a User's Identity. The user possesses the Credential and controls its use through one or other authentication protocols. A Credential may incorporate a password, cryptographic key or other form of secret.
- **Relying Parties** are the entities that provide online digital services to people with a Digital Identity. This can include government or private services. These Relying Parties consume Digital Identity to ensure certainty about the identity of the person they are interacting with.

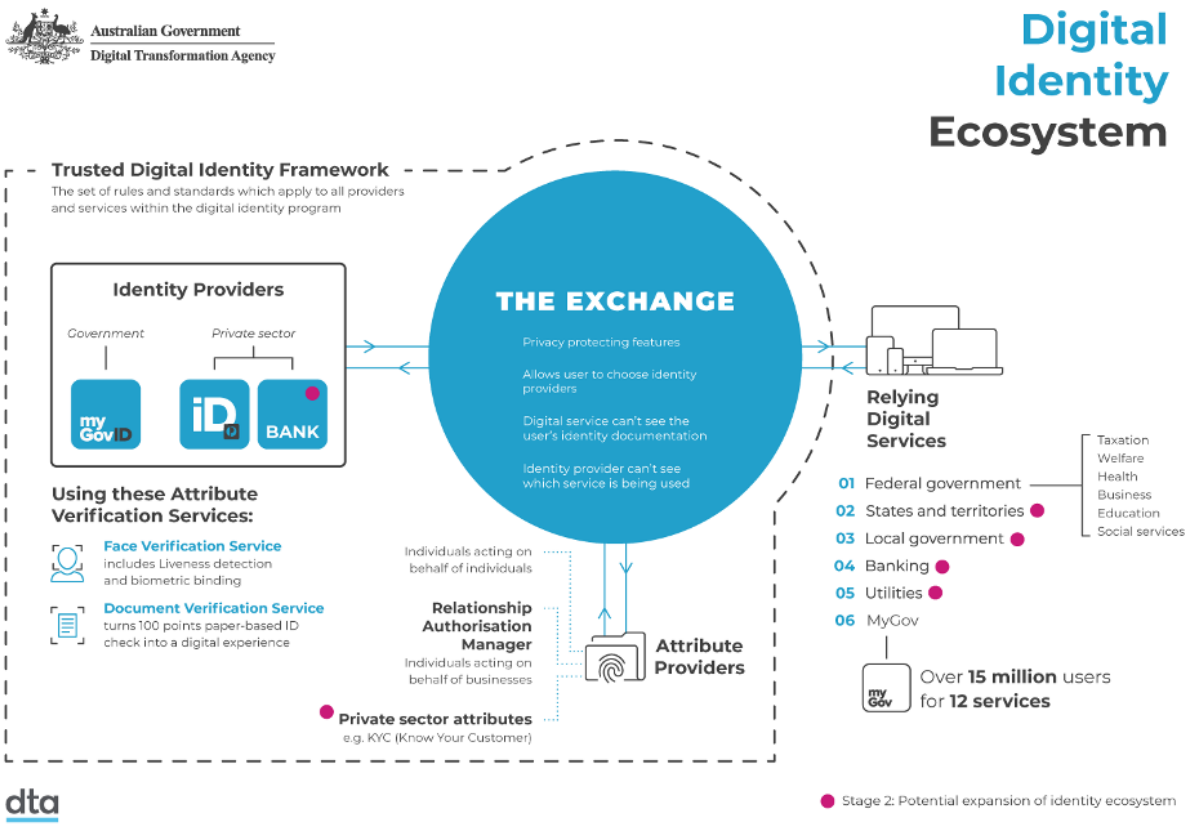
One important component of the Digital Identity system is the **Trusted Digital Identity Framework (TDIF)** which covers the accredited elements of the system, and is based on core principles relating to privacy, security and integrity.

All Participants in the Digital Identity System apart from Relying Parties are accredited against the TDIF.

The TDIF sets out requirements around privacy, fraud protection, security and identity proofing, which form the standards of the Digital Identity System those parties must meet. The TDIF also describes the technical details under which the federation operates.

Further information on the Trusted Digital Identity Framework (TDIF) is available from:

- <www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework>
- <www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework/framework-documents>
- <www.dta.gov.au/our-projects/digital-identity/digital-identity-glossary>



Australian Government
Digital Transformation Agency

Digital Identity Ecosystem

Trusted Digital Identity Framework
The set of rules and standards which apply to all providers and services within the digital identity program

Identity Providers
Government
Private sector

Using these Attribute Verification Services:

Face Verification Service
includes Liveness detection and biometric binding

Document Verification Service
turns 100 points paper-based ID check into a digital experience

THE EXCHANGE
Privacy protecting features
Allows user to choose identity providers
Digital service can't see the user's identity documentation
Identity provider can't see which service is being used

Individuals acting on behalf of individuals

Relationship Authorisation Manager
Individuals acting on behalf of businesses

● Private sector attributes
e.g. KYC (Know Your Customer)

Attribute Providers

Relying Digital Services

01 Federal government
02 States and territories ●
03 Local government ●
04 Banking ●
05 Utilities ●
06 MyGov

Taxation
Welfare
Health
Business
Education
Social services

Over **15 million** users for **12 services**

dta

● Stage 2: Potential expansion of identity ecosystem

Privacy and the Digital Identity System

The Digital Identity system has been the subject of two earlier PIAs:

- PIA1 (December 2016)
- PIA2 (September 2018)

These are available from <www.dta.gov.au/our-privacy-policy#privacy-impact-assessments>.

The DTA has commissioned a third PIA – and this PIA is being conducted in the broader context of the development of the Digital Identity system. This PIA considers elements that were not resolved in the first two PIAs and changes to both the TDIF and the governance aspects of the Digital Identity system that have occurred since the first two PIAs.

The development of the Digital Identity System introduced key privacy features into the technical design and policy settings.

The primary privacy feature was the decision to include specific privacy requirements in the accreditation regime – the TDIF. These requirements impose additional privacy protections beyond the baseline privacy protections in the Australian Privacy Principles (APPs) contained in the Commonwealth *Privacy Act 1988*.

These protections include:

- The Digital Identity System is an entirely voluntary system, designed to provide an alternative to paper-based identity verification processes. No Australian will be compelled to create a Digital Identity.
- The Digital Identity Program includes a commitment to maintaining a federated identity system, with multiple Identity Providers;
- The Digital Identity System allows users to have more than one Digital Identity (e.g., identities provided by different Identity providers or identities at different Proofing levels);
- The Trusted Digital Identity Framework (TDIF) requirements include a prohibition on use of a single identifier across the federation;
- The TDIF requirements include a prohibition on customer profiling across the federation;

- The TDIF requirements include restrictions on the use and retention of biometrics to those that a transparent and required for verification on the system;
- The TDIF requirements include a requirement for express consent from an individual or their representative to use the system to authenticate and pass attributes to a service;
- A technical ‘double blind’ design has been implemented that means Identity Providers and Relying Parties cannot see each other’s transactions;
- A user portal is being developed that will show recent transactions so consumers can recognise suspicious transactions; and
- All applications for TDIF accreditation must be accompanied by an independent Privacy Impact Assessment (PIA).

While the TDIF privacy requirements impose a rigorous privacy regime on system participants, the 2018 Privacy Impact Assessment of the Digital Identity System and TDIF recommended that the important protections in the TDIF privacy requirements be enshrined in legislation.

Note: Any potential legislative framework would be the subject of additional privacy consideration stakeholder consultation and is not the focus of the current PIA. Note: as of September 2020 the DTA was preparing a consultation paper on proposed legislation, and this was released in November 2020.[29]

[29] Refer to <haveyoursay.digitalidentity.gov.au/digital-identity>

Appendix 6 – Stakeholders

In consultation with the DTA, 29 stakeholder organisations were identified and invited to participate in consultation about the content of PIA3 – focussing around Nine Key Implementation Issues.

The stakeholders invited included:

- Academic/Expert
- Accredited TDIF Participant
- Consumer / Community Advocate
- Potential TDIF Participant
- Privacy Advocate
- Privacy Regulator

The 2020 'COVID' year proved challenging to engage with stakeholders – and Galexia adopted an online and PDF/DOCX survey – consulting both with DTA and a sample set of stakeholders over a period of four months to develop:

- A summary information pack – Refer to Appendix 5 – The Digital Identity System Background (as of July 2020).
- The online survey (or downloadable DOCX) – Refer to <dtaidentitypia.galexia.com>.

We have observed a level of stakeholder fatigue (not limited to TDIF/Digital Identity) across 2019/2020.

It can be challenging to achieve a balance in a few areas, with stakeholders considering they have:

- Too much / too little information
- Too much / too little consultation
- The pace is happening too quickly / too slowly

Additionally, it can be very challenging for stakeholders to understand the scope and complexity of the Digital Identity system and the detail of the TDIF document stack – the structure of which has changed extensively from TDIF3 to TDIF4. This is a challenge that DTA faces and has been improving public facing communications and stakeholder engagement.

Galexia took a flexible approach and extended responses to the survey to September 2020.

The following organisations responded to the survey/questionnaire (we have not identified individuals)

- Australian Communications Consumer Action Network (ACCAN) <accan.org.au>
- Australian Privacy Foundation (APF) <www.privacy.org.au>
- Office of the Australian Information Commissioner (OAIC) <www.oaic.gov.au>
- Office of the Victorian Information Commissioner (OVIC) <www.ovic.vic.gov.au>
- Queensland Office of the Information Commissioner (OIC) <www.oic.qld.gov.au>
- Services Australia Identity Exchange
- UNSW Law Faculty

Galexia sincerely thanks and recognises these organisations for the significant and meaningful contributions that were made.

Appendix 7 – 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>
CoI	Commencement of Identity	
CSP	Credential Service Provider	
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	
EDI	Evanescent Deterministic Identifier	
FMS	Face Matching Services	
FVS	Face Verification Service	
GUID	Globally Unique Identifier	
IdP	Identity Provider	
IOA	Interim Oversight Authority	
MOU	Memorandum of Understanding	
NDFLRS	National Driver Licence Facial Recognition Solution	
NIPG	National Identity Proofing Guidelines	
NISCG	National Identity Security Coordination Group	
NIST	National Institute of Standards and Technology (US Department of Commerce)	<www.nist.gov>
OA	Oversight Authority	
OAIC	Office of the Australian Information Commissioner	<www.oaic.gov.au>
OIDC	OpenID Connect	<openid.net/connect>
PIA	Privacy Impact Assessment	
PKI	Public Key Infrastructure	
PORO	Proof of Record Ownership	
RFID	Radio-frequency identification	
RP	Relying Party	
SAML	Security Assertion Markup Language	
TDIF	Trusted Digital Identity Framework	<www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework>

Appendix 8 – The Australian Privacy Principles (APPs)

Refer to Schedule 1 of *Privacy Act 1988* ((Cth)
<www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html> or
<www.legislation.gov.au/Details/C2020C00025>.

Part 1—Consideration of personal information privacy

APP 1 Australian Privacy Principle 1—open and transparent management of personal information[30]

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

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 Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

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 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(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.

Availability of APP privacy policy etc.

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.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

APP 2 Australian Privacy Principle 2—anonymity and pseudonymity[31]

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.

[30] OAIC Guidelines, *Chapter 1: APP 1 — Open and transparent management of personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

[31] OAIC Guidelines, *Chapter 2: APP 2 — Anonymity and pseudonymity*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity>.

Part 2—Collection of personal information

APP 3 Australian Privacy Principle 3—collection of solicited personal information[32]

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 This subclause applies in relation to sensitive information about an individual if:

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

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

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.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

[32] APP 3 sets out the requirements for the collection of personal information. The Office of the Australian Information Commissioner (OAIC) has issued guidelines on APP 3 that warn there are privacy risks associated with:

– Collecting personal information about a group of individuals, when information is only required for some of those individuals;
– Collecting more personal information than is required for a function or activity; or
– Collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future.

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.

More information: OAIC APP Guidelines, *Chapter 3: APP 3 — Collection of solicited personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

APP 4 Australian Privacy Principle 4—dealing with unsolicited personal information[33]

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

APP 5 Australian Privacy Principle 5—notification of the collection of personal information[34]

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:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) 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 by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the 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 notification or to otherwise make the individual aware of them.

[33] More information: OAIC APP Guidelines, *Chapter 4: APP 4 — Dealing with unsolicited personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information>.

[34] More information: OAIC APP Guidelines, *Chapter 5: APP 5 — Notification of the collection of personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>.

Part 3—Dealing with personal information

APP 6 Australian Privacy Principle 6—use or disclosure of personal information[35]

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.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

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

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; 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.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity’s primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

[35] The *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC) 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: OAIC APP Guidelines, *Chapter 6: APP 6 — Use or disclosure of personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

APP 7 Australian Privacy Principle 7—direct marketing[36]

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the ***first organisation***) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

[36] More information: OAIC APP Guidelines, *Chapter 7: APP 7 — Direct marketing*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing>.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(aa) Division 5 of Part 7B of the *Interactive Gambling Act 2001*;

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

APP 8 Australian Privacy Principle 8—cross-border disclosure of personal information[37]

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

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

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

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For ***permitted general situation***, see section 16A.

APP 9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers[38]

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

[37] More information: OAIC APP Guidelines, *Chapter 8: APP 8 — Cross-border disclosure of personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.

[38] More information: OAIC APP Guidelines, *Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers>.

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

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For ***permitted general situation***, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4—Integrity of personal information

APP 10 Australian Privacy Principle 10—quality of personal information[39]

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.

APP 11 Australian Privacy Principle 11—security of personal information[40]

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

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

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

[39] The *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC) 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: OAIC APP Guidelines, *Chapter 10: APP 10 — Quality of personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information>.

[40] 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:
– OAIC, *Guide to securing personal information*, 5 June 2018 <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information>.
– OAIC Guidelines, *Chapter 11: APP 11 — Security of personal information,* 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>.

Part 5—Access to, and correction of, personal information

APP 12 Australian Privacy Principle 12—access to personal information[41]

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.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(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) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

[41] More information: OAIC APP Guidelines, *Chapter 12: APP 12 — Access to personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information>.

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

APP 13 Australian Privacy Principle 13—correction of personal information[42]

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.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

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).

[42] The *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC) contain a set of hints and risks under the category of correction of personal information, including:
– Getting access to personal information should be clear and straightforward.
– Inaccurate information can cause problems for everyone!

More information: OAIC APP Guidelines, *Chapter 13: APP 13 — Correction of personal information*, 22 July 2019 <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information>.