Australian Government
Digital Transformation Agency

Privacy Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

Change log

Version	Date	Author	Description of the changes
0.01	Mar 2017	JS & DA	Initial version
0.02	May 2017	JS	Updates based on feedback from privacy stakeholders and internal feedback. Updates include: • Changed headings and restructure of the order of content. • Opt in privacy requirements. • Cross border and contractor disclosure. • Refinement to sections on reporting data breaches, definition of personal information, use and disclosure, consent, Privacy Impact Assessments and government identifiers. • Aligning Governance requirements to announcements about Australian Public Service Privacy Code.
0.03	Jul 2017	SJP	Minor updates to align with other Trust Framework documents
0.04	Sept 2017	JS	Removed Relying Party. Removal of list of metadata retained by the Exchange. Removal of minimal age limits. Minor updates to support the consultation draft.
0.05	Jan 2018	JS	Updates based on feedback from targeted and public consultation. Merged Privacy Audit document into Privacy Requirements. Aligned requirements to registered Australian Government Agencies Privacy Code.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **MUST NOT** – means an absolute prohibition of this document.
- **SHOULD** – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.
- **SHOULD NOT** – means there may exist valid reasons when a particular item is acceptable, but the full implications need to be understood before implementing the item.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

The CPRs apply whether an Applicant or Accredited Provider is subject to the *Privacy Act 1988* (Cth) (Privacy Act), state or territory privacy legislation or not covered by privacy law. These requirements rely heavily on the Australian Privacy Principles (APPs), other provisions in the Privacy Act and the Australian Government Agencies Privacy Code but are intended to be more specific and provide the highest standard across Australian and state government privacy legislation. The TDIF has incorporated relevant parts of the European Union General Data Protection Regulations (EU GDPR), particularly the consent requirements, but the TDIF does not seek to enforce the EU GDPRs.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

2 Part one: Privacy requirements

2.1 General requirements

Identity Exchanges **MUST** operate as separate legal entities to other identity federation participants and **MUST** establish and maintain its own privacy management arrangements.

The Applicant **MUST** comply with its obligations under the Privacy Act or, where relevant, state or territory privacy legislation and applicable Privacy Codes.

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 Trust Framework Accreditation[2].

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 metadata created in respect of the identity attributes collected by an Identity Exchange.
- The following privacy requirements apply to all Applicants unless explicitly stated otherwise. There are some requirements on Authorised Assessors under the heading Privacy Audit.

[2] This will be enforced by the Trust Framework Accreditation Authority

2.2 Privacy governance

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:
    - Handling of internal and external privacy enquiries, privacy complaints.
    - Requests for access to and correction of personal information made under the Privacy Requirements and privacy legislation.
    - Maintaining a record of the Accredited Providers personal information holdings.
    - Assisting with the preparation of Privacy Impact Assessments (PIAs).
    - Maintaining the Applicant's register of PIAs.
    - Measuring and documenting the Applicant's performance against the privacy management plan and updating privacy policies, at least annually.
- At all times, have a designated Privacy Champion responsible for:
    - Promoting a culture of privacy within the Applicant that values and protects personal information.
    - Providing leadership within the Applicant's organisation on broader strategic privacy issues.
    - Reviewing and approving the Applicant's privacy management plan, and documented reviews of the Applicant's progress against the privacy management plan.
    - 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.

2.2.2 Policies

The Applicant **MUST** publish a clearly expressed and up to date Privacy Policy[3] 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 APPs[4] and CPRs 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).

Privacy Policies **MUST** be regularly (at least annually) reviewed and updated.

The Applicant **MUST:**

- Develop and maintain a privacy management plan which identifies specific, measurable privacy goals and targets; and sets out how an Applicant take steps as are reasonable in the circumstances to implement practices, procedures and systems to implement the CPRs and other relevant privacy laws.
- Document the Applicant's performance against its privacy management plan at least annually.

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 Accredited Provider. The privacy education must address the privacy obligations of staff, and policies and procedures relating to privacy, particularly the CPRs.

[3] See *References* for further information on developing an APP Privacy Policy.

[4] Or particular jurisdictional Privacy Principle.

- 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 the CPRs and privacy laws.
- Monitor compliance with its privacy practices, procedures and systems regularly.

2.3 Privacy Impact Assessment

As part of the Trust Framework Accreditation Process, the Applicant:

- **MUST** commission a PIA, by an Authorised Assessor to review the privacy impacts of the Applicant's identity service.
    - An Authorised Assessor is an independent consultant which is a separate legal entity to the Applicant and not under its control.
- **MUST** conduct a PIA for all high privacy risk projects related to its identity service.
    - 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 responses.
- **MUST** publish the register, or a version of the register, on its website.

A PIA **SHOULD** be conducted using the *Guide to undertaking privacy impact assessments*[5].

[5] See *References* for further information on undertaking a PIA.

A PIA **MUST** at a minimum:

- Be conducted by an Authorised Assessor with knowledge and experience in conducting PIAs.
- 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:
    - Risks of non-compliance with the relevant laws related to privacy.
    - Risks of non-compliance with the CPRs.
    - The impact of the project on individuals.
    - Whether privacy impacts are necessary or avoidable.
    - Possible mitigation of risks.
- Provide recommendations to the Trust Framework Accreditation Authority.

2.4 Data Breach Response Management

The Applicant **MUST**:

- Gave a documented Data Breach Response Plan (see below).
- For Applicants covered by the *Privacy Act 1988,* report serious data breaches to individuals and the Information Commissioner as required under the *Privacy Act 1988*[6] and also report the data breach to the Trust Framework Accreditation Authority.
- For Applicants not covered by the the *Privacy Act 1988,* report serious data breaches to individuals as described in the *Privacy Act 1988* and also report the data breach to the Trust Framework Accreditation Authority.

[6] See www.legislation.gov.au/Details/C2017A00012 for further information.

The Data Breach Response Plan[7] 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[8].

2.5 Notice of Collection

The Applicant **MUST**, when it collects personal information of users, 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).

[7] See *References* for further information on developing a Data Breach Response Plan.

[8] See *Trust Framework: Protective Security Requirements* for further information on developing an Incident Response Plan.

2.6 Collection and use limitation

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.
- It only collects information by lawful and fair means.
- It only collect 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 consents to his/her identity attributes being disclosed at the time he/she verifies to a new 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).

The Applicant **MUST NOT** use personal information for direct marketing purposes. Excluding uses and disclosures relating to identity verification, which requires consent, and direct marketing, which is prohibited, other uses and disclosures **MUST** comply with the APPs[9].

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.

[9] See Australian Privacy Principle 6 at www.legislation.gov.au/Details/C2017C00283

2.7 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 verify an individual's attributes (for example matching a person's face to a photo document):

- **MUST NOT** be used for any other purpose.
- **MUST NOT** be disclosed to a third party.
- **MUST** be destroyed once the verification process has concluded.

2.8 Consent

An individual **MUST** consent to his/her personal information being disclosed prior to he/she verifying to a new Relying Party. For consent to collections, uses and disclosures of personal information to be valid the following conditions **MUST** be satisfied:

- 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.

Consent **MUST** be given explicitly.

An individual **MUST** be made aware of the implications of providing or withholding consent.

The Applicant **MUST** ensure that an individual is properly and clearly informed (without legal or industry jargon) about how their personal information will be handled.

An individual **MUST** have the capacity to consent.

If an Applicant is uncertain as to whether an individual has capacity to consent at a particular time, it **SHOULD NOT** rely on any statement of consent given by the individual at that time.

Note: in an online environment consent can be established where an individual electronically consents, what is being consented to is clear and identity documents reflect a user's age.

Consent given at a particular time in particular circumstances **MUST NOT** be assumed to endure indefinitely.
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.

2.8.1 Identity Service Provider additional requirements

If the Applicant is an Identity Service Provider it **MUST**:

- Seek and obtain consent to verification of identity attributes 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.

2.9 Cross border and contractor disclosure

Applicants **MUST** comply with APP 8 - cross border disclosure of personal information[10].

In addition, before an Applicant discloses personal information to an overseas recipient (for example an overseas cloud host) or a contracted service provider, the Applicant **MUST** take such steps that are reasonable to ensure the recipient only uses the information for purposes related to identity verification.

[10] See Australian Privacy Principle 8 at www.legislation.gov.au/Details/C2017C00283

The Applicant **MUST** ensure it has an enforceable contractual arrangement with the overseas recipient or contracted service provider that specify:

- The purpose/s for which the overseas recipient or contracted service provider are permitted to use or disclose the personal information.
- The minimum technical and organisational measures that will apply to ensure the security of the personal information that the Applicant owns and controls the information, including specifying that it can request that the overseas party or contracted service provider destroy the information.
- Mechanisms that enable the Applicant to monitor compliance with these arrangements.

If an Applicant contracts the operation of a part of its business that relates to the TDIF it **MUST** make compliance with these CPRs a term of the contract and that the third party can be audited by the Trust Framework Accreditation Authority.

See the *Trust Framework: Protective Security Requirements* for more information on security and contract management.

2.10 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 (ie an identifier that is sent to more than one Relying Party or Identity Service Provider).

2.11 Access, correction and dashboard

2.11.1 Access

The Applicant **MUST**:

- Where it holds personal information about an individual, on request by the individual, give the individual access to the information.
    - 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.

2.11.2 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.

2.11.3 Dashboard

If the Applicant is an Identity Exchange it **MUST** provide individuals with access to the metadata on transactions it logs (ie that has not been deleted under its destruction policy) in a dashboard format.

> **Note:** an Identity Exchange will not be able to directly identify an individual and therefore the individual will need to access its metadata by logging on through an Identity Service Provider.

2.12 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.

2.12.1 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.

2.13 Handling Privacy Complaints[11]

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 CPRs 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.

[11] See *References* for further information on handling privacy complaints in organisations.

- 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.

2.14 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:
  - Whether stored personal information needs to be retained under law or a court/tribunal order.
  - Data retention timeframes.
  - De-identification policies and practices (including mitigation of the risk of re-identification).
  - 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.

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 Authorised Assessors when conducting the privacy audit as part of the Trust Framework Accreditation Process.

The privacy audit is required after the Applicant has performed a PIA and submitted evidence to the Trust Framework Accreditation Authority to address the CPRs.

The aim of the privacy audit is to:

- Determine whether the Applicant can demonstrate it has complied with the CPRs.
- Determine whether the Applicant has addressed all recommendations arising from the PIA.
- Document the results of the privacy audit in a report to the Trust Framework Accreditation Authority.

The following activities have occurred by the time the privacy audit is undertaken:

- The Applicant has provided the Trust Framework Accreditation Authority with a plan demonstrating how they will meet the CPRs.
- The Applicant has provided the Trust Framework 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 Trust Framework Accreditation Authority with a report which outlines how and by when they will address the recommendations outlined in the PIA.
- As part of the Trust Framework Accreditation Process the Applicant has submitted protective security, risk management and fraud control documentation to the Trust Framework Accreditation Authority. This provides additional context to the privacy audit.

3.2 Privacy audit process

The Authorised Assessor **MUST** carry out the following steps as part of the privacy audit:

- Evaluate assessments or comments already made by the Trust Framework Accreditation Authority.
- Evaluate all relevant evidence provided by the Applicant to the Trust Framework 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:
    - Documentation reviews.
    - Conduct a site visit.
    - Interview key privacy and operations personnel.
- The Authorised Assessor **MUST** retain evidence to support its findings. The Authorised Assessor will only need to provide evidence indicated in the privacy audit tool below to the Trust Framework 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.
- Provide a report of findings (see *Annex A: privacy audit template* below) to the Trust Framework Accreditation Authority. The report **MUST** at a minimum:
    - Summarise the activities performed during the privacy audit.
    - Advising whether or not the Applicant has complied with the TDIF CPRs, including any requirements that could not be adequately assessed due to access or timing issues.
    - Recommends remediation actions to address any areas of non-compliance.
    - Include the Applicant's response to the privacy audit findings and recommendations.

3.3 Type of audit and auditor's skills

The privacy audit is to determine whether the Applicant is compliant with the TDIF CPRs and has addressed the PIA recommendations. The Authorised Assessor **MUST NOT** take a 'tick box' approach to the requirements.

The Applicant **MUST:**

- Employ an Authorised Assessor to carry out the privacy audit, who can either an internal auditor or they can procure the services of an external auditor to carry out the privacy audit.
- Ensure the auditor has adequate experience and training in auditing to carry out the privacy audit.
- Ensure the auditor has adequate experience and knowledge of privacy.
- Ensure the auditor is sufficiently independent from the Applicant's identity service.

3.4 Privacy audit roles and responsibilities

3.4.1 Trust Framework Accreditation Authority

The Trust Framework Accreditation Authority is responsible for:

- Ensuring that the accreditation process is conducted with due care and in accordance with the published Trust Framework documents.
- Reviewing, within agreed timeframes, all relevant Applicant documentation to ensure conformance to the published Trust Framework documents.
- Providing relevant documentation, it holds on an Applicant to the auditor.
- Considering all reports and recommendations from Authorised 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.
- Responding to the auditor and Trust Framework Accreditation Authority regarding proposed remediation activities and timeframes.
- Remediating all identified non-compliance issues to the satisfaction of the Trust Framework Accreditation Authority.

3.4.3 Authorised Assessor

The Authorised Assessor is responsible for:

- Assessing the Applicant's compliance against the CPRs.
- Documenting their findings, which:
- Summarise the activities performed during the evaluation.
- Suggest remediation actions to address areas of non-compliance or unmitigated risk.
- Recommend whether or not the Applicant has satisfied the TDIF CPRs.
- Providing their findings to the Trust Framework Accreditation Authority.

References

The following information sources have been used in developing this document.

1. Bradner, S. 1997, 'Key words for use in RFCs to Indicate Requirements Level' (Requests for Comment 2119), Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119
2. Commonwealth Ombudsman, 2017, 'better practice guides', Australian Government, Canberra. http://www.ombudsman.gov.au/publications/better-practice-guides
3. Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments', Australian Government, Canberra.
4. Office of the Australian Information Commissioner, 2014, 'Guide to developing an APP privacy policy', Australian Government, Canberra.
5. Office of the Australian Information Commissioner, 2016, 'Guide to developing a data breach response plan', Australian Government, Canberra.
6. Privacy Act 1988 (Cwth)
7. Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cwth)
8. Standards Australia, 2014, 'Guidelines for complaint management in organisations (AS/NZS 10002:2014)', Standards Australia & New Zealand, Sydney & Wellington

Annex A: Privacy audit template

Trusted Digital Identity Framework – Privacy audit		
Date of audit:		
Date of audit report:		
Name of auditor:		
Summary of activities performed during the privacy audit: • 1 • 2 • 3		
Remediation actions and other notes • Add remediation actions to each Privacy Requirement where there is a non-compliance • Add notes the Trust Framework Accreditation Authority should be made aware of		
Privacy Requirement **PIA Recommendation**	**compliance** **non-compliance**	**Required attachment** **Accreditation Authority notes**
Privacy Governance		
Privacy Impact Assessment		
Data Breach Response Management		
Notice of Collection		
Collection and use limitation		
Consent		
Cross border and contractor disclosure		
Government Identifiers		
Access, correction and dashboard		
Quality of personal information		
Handling of privacy complaints		
Destruction and de-identification		
PIA recommendations		