PRIVACY IMPACT ASSESSMENTS (PIAs)

Threshold Assessments

Privacy Impact Assessments (PIAs) and PIA Threshold Assessments

A Privacy Impact Assessment (PIA) is used to assess and identify privacy risks of a project or business activity, and to ensure that CMTEDD's handling of the personal information will:

- be compliant with the *Information Privacy Act 2014*, and the Territory Privacy Principles (TPPs);
- consider any broader privacy implications and risks; and
- identify any stakeholder concerns or issues about how personal information will be handled by the proposed projects or business activities.

It is best privacy practice to undertake a PIA Threshold Assessment, and if required a full PIA at the earliest opportunity when:

- undertaking a new project or business activity that collects personal or sensitive information, and
- when making changes to the way in which personal and sensitive information is collected, used or disclosed, stored and secured in existing projects or business activities.

PIA's are living documents and can be updated, or regularly reviewed to ensure CMTEDD's privacy obligations are being met throughout the life of a project or program.

When do I need to undertake a PIA Threshold Assessment?

Undertaking a PIA Threshold Assessment is the first step in determining if a full PIA is enquired or not.

If the information you are proposing to collect, store, use or disclose ***does not*** include or contain personal information, or does not change an existing information handling practice (that has previously been assessed) then ***you do not need*** to undertake a PIA Threshold Assessment.

If the information you are proposed to collection, store, use or disclose ***does*** contain personal information, and you are:

- collecting that information for a new project or business activity;
- changing an information handling practice for an existing project or business activity; or
- collecting a new kind of personal information as part of your project or business activity;

you ***will need*** to undertake a PIA Threshold Assessment as the first step.

Depending on the outcome of the PIA Threshold Assessment you may then need to undertake a full PIA. There are no rules about whether a full PIA will be necessary, and each project must be considered on a case-by-case basis.

Not all projects will require a full PIA, and those that do may only require a brief PIA where there is little personal information being handled, or only minor changes to information handling practices.

Benefits of undertaking a PIA Threshold Assessment

PIA Threshold Assessments can be beneficial in a number of ways including:

- raising privacy awareness early in the life of a project or proposed change to a program;
- building in privacy by design; and
- reducing legal, operational and reputational issues, risks and costs.

By identifying the privacy risks and issues early, appropriate risk mitigation or treatments can be adequately planned for and put in place to protect personal privacy and personal information.

What about de-identified personal information?

A PIA Threshold Assessment is still advised even if it appears that there is little to no risk. For example, if the personal information is to be de-identified and is considered to no longer be personal information.

There is never no risk when dealing with de-identified personal information, and consideration must be given to the possible re-identification of the individuals. Re-identification can occur when data that is already in the public domain can be used or accessed in combination with the de-identified data you are proposing to make public, to potentially re-identify an individual.

For more practical guidance on de-identification of personal information and data, please refer to the resource that was published in partnership with CSIRO, Data61 and the OAIC on the CSIRO's website, that provides A framework for data de-identification and an associated report, The De-identification Decision Making Framework and appendices.

Consultation and other resources

In addition, review is recommended of the following business unit's policies, and consultation (if required), to ensure that you have adequately considered other related risks and issues that may intersect with privacy risks and issues:

- Shared Services;
  - Access control policy;
  - ICT Security Policy;
  - ICT Security Risk Management Standard;
  - Security advice for cloud procurement; and
  - Cloud Security Assessment.
- Corporate;
  - CMTEDD Risk Management Plan; and
  - CMTEDD Risk Management Framework and Policy.

CMTEDD's PIA Threshold Assessment tool

This assessment tool is designed to assist CMTEDD staff to identify major privacy risks and inform project staff if a full PIA is recommended. PIA's are not mandatory but are considered to be best privacy practice and assist with:

- good privacy governance;
- project management;
- managing personal information as a valuable business asset through the information life cycle; and
- can aid in the management of privacy breaches, particularly identifying gaps or weakness in business processes that may have contributed to the breach.

CMTEDD Privacy Officer review and clearance

Please submit your completed PIA Threshold Assessment tool to the:

CMTEDD Privacy Contact Officer

Phone: 02 6207 8175

Email: CMTEDDPrivacy@act.gov.au

Where to find more information?

If you have any questions about this fact sheet or have a question about PIA Threshold Assessments that is not answered here, please contact the CMTEDD Privacy Contact Officer on the details above, or visit the OAIC's website for more detailed information and Privacy Impact Assessment eLearning course.

PIA Threshold Assessment Checklist

Title of project	
Brief description of the project:	The Traffic Camera Expansion (TCE) is a government initiative aimed at expanding the existing camera network, including both road and Mobile Device Detection Camera, in a staged approach. Phase 1, which began on August 27, 2024, focuses on issuing infringements for unregistered vehicles in the ACT. Phase 2, currently in preparation, will target infringements related to seatbelt non-compliance.

Questions	Yes	No	N/A	Please describe
1. Is this a new project, business activity or program?		No		*If yes, please describe how personal information will be handled and secured i.e. method of collection, storage, use and disclosure of personal information* This is not a new project but rather Phase 2 of an ongoing TCE project aimed at delivering a new pathway for issuing seatbelt non-compliance infringements using the existing Mobile Device Detection Camera (MDDC). The MDDCs will detect seatbelt non-compliance events and capture images which will then be used in the adjudication process to issue infringements. The MDDC system is provided by Acusensus Australia Pty Ltd (Acusensus) and will integrate with: • Xilium (the adjudication system) delivered by Sensys Gatso Australia Pty Ltd (Gatso); • Rego.ACT system; and Access Canberra web portal will integrate with Xilium. MDDC PIAs undertaken in 2020 and 2023 outline the actions taken for management of personal information and recommendations to ensure adequate protections are in place. Recommendation 3 (PIA 2023) states: *"If there are any material changes to the information flows identified in Schedule 1, including any proposed new use cases regarding the use of MDDC System data and images (such as the detection and enforcement of laws relating to offences other than driver mobile device use), we recommend the CMTEDD undertake:* *• a privacy threshold assessment; and*

				• *if required, further assessment of privacy impacts and compliance risks (which could be in the form of a supplementary PIA). "* Given that we will be using MDDC data and images for enforcing laws related to offences other than driver mobile device use, we consider that privacy threshold assessment is necessary.
2. Does the project propose to collect personal information?	Yes			*If yes, please give examples of information collected e.g. name or email address*
○ Does the project propose to collect sensitive information (including biometric information)?	Yes			*If yes, please give examples of information collected e.g. criminal record or photographs* Photographs
○ Does the project propose to collect health information?		No		*If yes, please give examples of information collected e.g. medical conditions* Unless the offender has a medical condition, they might be exempt but will need to provide proof of their medical condition through a review process.
3. If this is an existing business activity or program, are you proposing to modify an existing information handling practice of personal information?		No		*If yes, describe how the new method will handle and secure the personal information, e.g. the method of collection is being changed from paper based forms, to electronic forms. If no, describe the current practices and why they do not need to be changed* No change to current practice. We will use the same process of enforcement as we use for speeding and mobile driver distraction offences. Facial features of a driver or passenger will be redacted where the image or individual is not relevant to the offence.
4. What is the main business function or 'primary purpose' which permits the collection of personal information (new or existing)?				*Describe the business purpose in brief* • Images collected through MDDC are currently used for the purpose of issuing infringements for using mobile device while driving a vehicle. • TCE Phase 2 will collect images through MDDC to identify seatbelt non-compliance and issue corresponding infringements.

5. Is the collection authorised or required by law?	Yes			*If yes, please state the name of the Bill/Act, and relevant sections. If no, what is currently in place that permits collection e.g. current administrative practices* The Collection is authorised by the following Acts. • *Information Privacy Act 2014* • *Road Transport (Safety and Traffic Management) Amendment Act 2021, S 24.*
6. Do any secrecy provisions apply to the access, collection, use and disclosure of the personal information?	Yes			*If yes, please specify section/Act* • *Road Transport (Safety and Traffic Management) Amendment Act 2021, S 29.*
7. How will the collection of the personal information affect the individual?				*Please provide details in brief about the type of activities the personal information will be used for e.g. imposition of fines or enforcement activities, or to take other actions against the individual?* Images of individuals not complying with seatbelt requirements will be collected through MDDCs. These images will undergo an adjudication process to determine if an offence has occurred. If the evidence confirms the offence, an infringement notice will be issued to the registered owner of the vehicle. Personal information will be used for activities such as issuing infringements, enforcement actions, and other measures against individuals who violate seatbelt requirements
8. Has any community consultation already been held to explore the privacy risks and perceptions of the public?		No		*If yes, what were the key privacy concerns or issues raised*

9. Will any personal information be subject to cross border disclosure?	No	*If yes, please provide details in brief what countries the information is being disclosed to* Assuming Cross Border means outside international borders
10. Will any personal information be stored in an offshore cloud?	No	*If yes, please provide details in brief about the cloud and which country it is in, and how the information will be uploaded i.e. what encryption or security measures will be applied. If no, and the cloud is in Australia, please name the cloud*
Who are the internal stakeholders?	*Please specify e.g. another business unit, legal team or contractors* • Infringement Review - Fair Trading and Compliance team • Digital, Design and Delivery team • Licensing and Registration team • Gatso • Acusensus	
Who are the external stakeholders?	*Please specify e.g. customers or general public* General public	

Data Matching

Note: If the personal information is being collected for a data matching purpose and the number of records matched is over 5000 annually, either in one bulk data transfer or cumulatively via several smaller data transactions, then you will need to consider if you should prepare a Data Matching Protocol in accordance with the OAIC guidelines on data matching, you may also still be required to undertake a full PIA as well.

If the data matching exercise is only a pilot, and if you are proposing to 'use/disclose' the personal information matched to take an administrative or punitive action, then natural justice must be afforded and the individuals affected provided with sufficient and specific notice (even after the collection).

Questions	**Please describe**
1. Is the personal information being collected for a data matching purpose?	*If Yes, complete the following section. If no, STOP HERE you do not need to complete the following section.* No

2.	Who owns the other data set?	Not applicable
3.	Are the owner of the data set an internal or external agency?	Not applicable
4.	*What other data set is the data matching with and*	Not applicable
5.	Are there other sensitivities around the data matching exercise i.e. public interest/concerns?	Not applicable

If you answered **YES** to any of the questions under 'Data Matching', you will need to undertake a full PIA, and you will also need to possibly develop a Data Matching Protocol.

Please discuss with the CMTEDD Privacy Contact Officer, or refer to the OAIC's website for some general advice and general principles on data matching available in the voluntary Guidelines on Data Matching in Australian Government Administration for more information.

CMTEDD Privacy Officer review and clearance

Please submit your PIA Threshold Assessment to the:

CMTEDD Privacy Contact Officer

Phone: 02 62078175

Email: CMTEDDPrivacy@act.gov.au

PIA Threshold Outcome

Full PIA is **not** required

Recommendations

The following analysis and recommendations about the privacy issues, or possible risk mitigation strategies and treatments includes:

No additional privacy risks are identified, TPP5 (notification of collection) and TPP6 (use or disclosure) may require some work in terms of updating policy, procedure, website etc information to notify the public of the

collection purpose which now includes seatbelt adherence. Signage on MDDC may need to be updated to show current use if it only mentions mobile devices.

Cleared by CMTEDD Privacy Officer

Name: Heather Johnston

Date: 16/10/2024