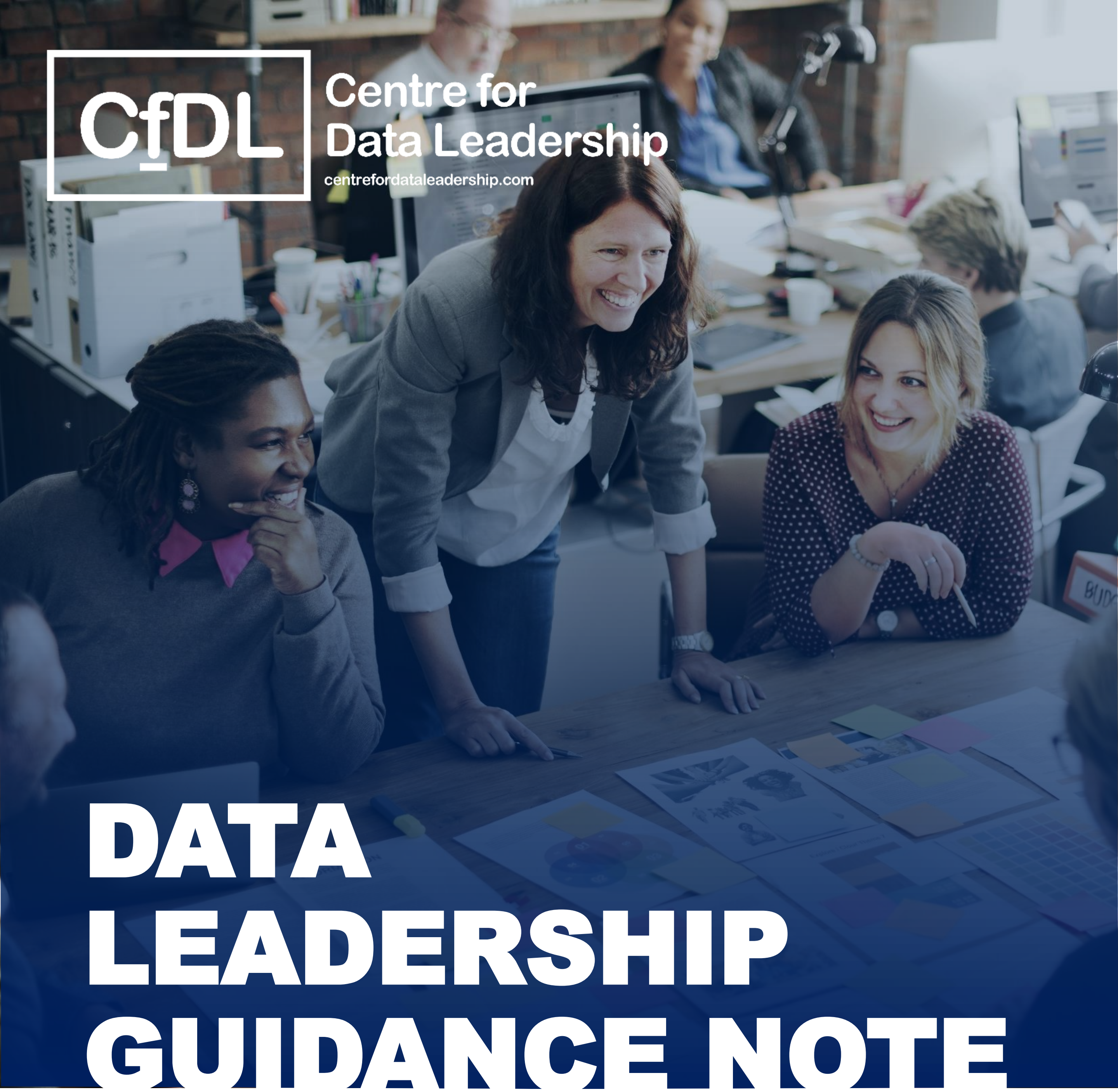


CfDL Centre for Data Leadership
centrefordataleadership.com

DATA LEADERSHIP GUIDANCE NOTE

Privacy Impact Assessment

April 2020

Powered by

SmartCitiesCouncil
Australia New Zealand

About us

SmartCitiesCouncil®
Australia New Zealand

Smart Cities Council Australia New Zealand (SCCANZ) is part of the Smart Cities Council, the world's largest network of smart cities companies, practitioners and policy makers, embracing technology, data and intelligent design to accelerate liveability, workability and sustainability in our cities and towns.

Further information about the Smart Cities Council can be found here.

Acknowledgements

GROUND UP
Consulting

This guidance note was developed in collaboration with our Associate Partner, Ground Up Consulting.

Ground Up Consulting specialises in enhancing knowledge and practice around privacy and the protection of personal information. The company offers niche privacy capacity building services for business, government and not for profit organisations through seminars, privacy induction training, targeted workshops and executive sessions.

Introduction

The privacy context

Overview

This Guidance Note provides an overview of Privacy Impact Assessment (PIA) for Cities, and outlines the fundamentals, benefits and key steps in undertaking a PIA.

It is intended to assist local governments in managing privacy around new projects and initiatives.

What is Privacy?

Privacy is often characterised in terms of rights or freedoms of a person, such as the right to be 'let alone' or be free from intrusion into one's personal life. From a practical perspective for Cities, privacy is the protection of personal information in accordance with the law while remaining mindful of community expectations.

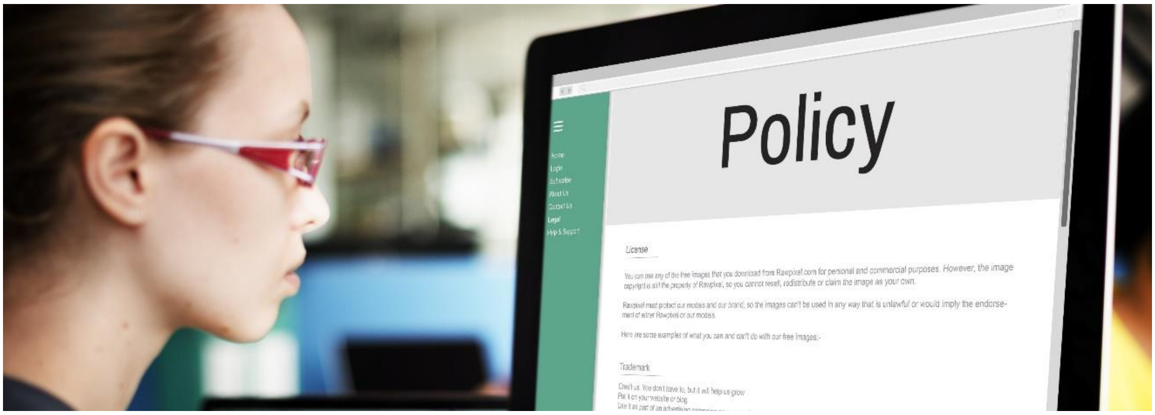
New Zealand and Australian states and territories each have privacy laws that include principles for how personal information is to be handled throughout its lifecycle. These principles inform and guide how Cities collect, use, store, secure, disclose and otherwise manage personal information.

Broadly, personal information includes information that identifies (or could lead to the identification of) an individual. A helpful diagram to help Cities unpack what is/is not personal information is here.

Cities require personal information to support many administrative and service delivery functions, in both digital and analogue contexts. For example, consider the personal information required to manage rates, local laws enforcement, community complaints, library borrowing and public consultations. And imagine development applications, community access to services and City employee management.

In addition, new technologies, applications, platforms and emerging evidence-based decision making (i.e., data analytics) processes increasingly involve personal information.

The Fundamentals



What is a Privacy Impact Assessment?

A PIA is an effective tool that Cities can use to assess the impacts a project may have on privacy and to make recommendations for addressing the impacts to the greatest extent possible.

It is a formal and deliberate due diligence exercise, where a project is evaluated from the perspective of privacy risk to ensure compliance with privacy obligations (as set out in the applicable privacy law) *and* demonstrate responsiveness to community privacy expectations.

When to do a Privacy Impact Assessment?

Cities should consider privacy obligations (and the risk of potentially not meeting those obligations) before designing and implementing new technologies, projects and initiatives, where it is proposed to make a significant change to how personal information is currently being managed and/or where the community has expressed privacy concerns.

Advice from privacy regulators in New Zealand, Australia and globally is that a PIA should be considered for the following:

- New or amended programs, activities, systems or databases
- New methods or procedures for information handling
- New or amended legislation
- Policy proposals
- Changes to how personal information is stored.

A PIA should be completed as soon as possible in the design of a new project. This will ensure that privacy is appropriately ‘baked in’ to the project, as opposed to being ‘bolted on’ a later stage.

Benefits of a Privacy Impact Assessment

Privacy regulators have identified many potential benefits of conducting a PIA, all of which are relevant to Cities.

The benefits include:

- Ensure projects are compliant with applicable privacy (and other) legislation
- Ensure projects reflect community privacy values and expectations
- Provide a comprehensive understanding of how projects will handle personal information
- Identify strategies for managing, minimising or removing privacy risks
- Minimise future risks and associated costs, time, and negative exposure
- Demonstrate to stakeholders and the community that privacy considerations have been built into projects
- Provide opportunity to increase community awareness of projects through avenues such as public consultation, information sessions and publications
- Promote internal privacy awareness and understanding of privacy issues both broadly and with respect to specific projects
- Assist in improving broader risk management processes.

Privacy Impact Assessment Process

The key steps

Cities need to ensure they establish their own policies and processes for conducting PIAs. The following key steps are provided to help guide that process.

Step 1. Threshold Assessment

Not all projects will require a PIA to be undertaken. A threshold assessment will identify if the project will involve personal information or if there is a privacy concern in the community (answering ‘yes’ to either question will likely trigger a PIA).

Before starting a PIA, Cities need to first determine whether a PIA is required. This is best done by completing a Privacy Threshold Assessment which includes, at a minimum, the following:

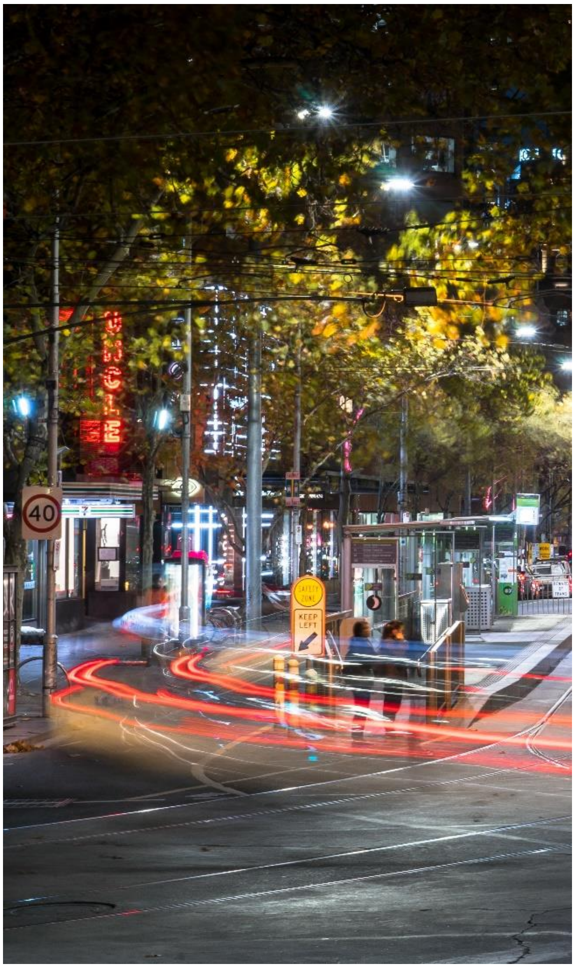
- Details of the project ‘owner’ or Project Manager
- A brief description of the project
- Whether (and to what extent) personal information is involved in the project
- Whether there is (or could be) privacy concern in the community about the project
- Whether a PIA is recommended
- Who is responsible for deciding whether and how to take next steps in the PIA process.

Step 2. Planning the PIA
Outline who will conduct the assessment (consider whether to conduct the PIA internally or use the services of an independent privacy advisor) and other relevant matters such as timeframe, budget, and whether to consult with the community.

Step 3. Describe the Project
It is important to know the purpose of the project and how it fits in with the City's objectives. Other relevant matters include the scope and extent of the project, how the project links with other programs or projects and who is responsible for the project.

Step 4. Identify and Consult with Stakeholders
Often Cities will be able to identify previously unknown privacy impacts through consultation with stakeholders. Seek the views of those who may be impacted by the project, such as internal business streams (e.g. information security team or intergovernmental relations), the community, regulatory authorities, contracted service providers and vendors.

Step 5. Map Information Flows
Describe and map the flow of personal information within the project. This is a visual representation of what happens to personal information, such as who will have access to it and how it will be collected, used, disclosed, stored and secured.



Step 6. Privacy Impact Analysis and Compliance Check
Conduct a deep-dive analysis of how the project complies with the applicable privacy law (and, potentially, other laws) and responds to community privacy expectations.

Step 7. Privacy Management – Addressing Risks
Often there are less privacy-invasive ways to achieve a project's goal. It is important to consider this, and whether there are opportunities to remove, mitigate or otherwise manage privacy risks that have been identified.

Step 8. Recommendations
It is important that recommendations are an honest accounting of how a project can improve its privacy position. Where risks have been identified, recommendations should focus on meaningful opportunities to address these.

Step 9. Report
A PIA Report is a methodical approach to displaying all of the information relating to the PIA process. It is intended to show the privacy risks and related recommendations in a way that can be both understood and actioned by City decision-makers.

Step 10. Respond and Review
A PIA is not a 'set and forget' process. The City should respond to each of the recommendations included in the PIA Report and, if required, conduct a further PIA for the project at a later point in the project timeline.

Additional Resources

This material has benefitted from the extensive guidance material made available by privacy regulators in the Australia and New Zealand region and globally. Particularly thanks to:

- New Zealand Privacy Commissioner: New Zealand Privacy Act
- Office of the Australian Information Commissioner: Australian Privacy Act, and the Privacy Act for each State and Territory
- New Zealand Privacy Commissioner: Privacy Impact Assessment Toolkit
- Office of the Australian Information Commissioner: Guide to Undertaking Privacy Impact Assessments
- Office of the Information Commissioner Northern Territory: Privacy Impact Assessment Guidelines
- Office of the Information Commissioner Queensland: Undertaking a Privacy Impact Assessment
- Office of the Victorian Information Commissioner: Privacy Impact Assessments
- Information and Privacy Commissioner New South Wales: Guide to Privacy Impact Assessments in NSW

We thrive on feedback and would welcome your comments to help make this work as impactful as possible. Please contact us at anytime.

engagement@anz.smartcitiescouncil.com
www.anz.smartcitiescouncil.com
@smartcitiesanz

Smart
Cities
Council
Australia New Zealand

Liveability | Workability | Sustainability