NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

IR-01-22-37552

12 January 2023

J A Harris
fyi-request-21326-4119124d@requests.fyi.org.nz

Request for information

Thank you for your Official Information Act request of 3 December 2022, asking

> *Please provide details of any guidelines and copies of any documents that guide when and why a privacy impact assessment needs to be completed, and how to complete a privacy impact assessment.*
>
> *Please provide details of privacy impact assessments developed/completed by Police. It is Not necessary to provide the content of the assessments themselves, just the number and subject of the PIA where an assessment was done.*

I note that your request for a list of PIAs was subsequently clarified to PIAs completed in the 2022 calendar year.

In response to your request, please find attached a copy of Police's TenOne internal guidance relating to Privacy Impact Assessment and Privacy by Design.

Further, please see below a table of PIAs completed in the 2022 calendar year.

PIA	Subject
1.	Ingestion of Sovereign Citizen Information into ArcGIS Enterprise
2.	Ingestion of Persons of Interest data into ArcGIS Enterprise
3.	Ingestion of Gang Activity and Offence Information into ArcGIS
4.	Ingestion of Bail Management data into ArcGIS Enterprise
5.	Arms Information System (AIS) – Release 1
6.	Visitor Management System (VMS)
7.	Hybrid email solution - Microsoft 365
8.	Unstructured text search across NIA attachments and narratives
9.	Rural Lookout Strategic Dashboard ArcGIS Enterprise
10.	Use of body worn cameras (in relation to use of Taser)
11.	Improvement of Mental Health Triage Line
12.	Use of Mail Chimp for tracking stakeholder engagement
13.	Voice of Customer platform use
14.	Trial use of dashcam technology
15.	Employee expense management software
16.	Financial Intelligence Unit Service Delivery Transformation
17.	Use of Citizen Space consultation platform
18.	IMS Photo Manager facial comparison system
19.	Motor Vehicle staff travel remediation project
20.	Personal information management - He Aranga Ake

I trust the information provided addresses your areas of interest.

Ngā mihi

Annabel Fordham
Chief Privacy Officer

TEN ONE

Privacy Impact Assessment and Privacy by Design

Personal information is a strategic Police asset in the delivery of Our Business. Good stewardship of personal information helps us maintain public trust and confidence.

Completing Privacy Impact Assessments (PIA) and using a Privacy by Design (PbD) approach go hand in hand to identify and design out privacy risk in Police systems and processes.

Good stewardship of personal information is enhanced by undertaking a PIA when a new project or way of handling personal information may affect privacy. Privacy by Design has an enduring effect – it means systems and processes are built to make it easier for our people to do the right thing and harder for them to make mistakes.

The PIA template is designed to be straightforward for project teams to complete and provides an opportunity for substantive comments and explanation of risks and mitigations. Privacy by Design means considering privacy from the beginning of a project, making safe information handling part of project thinking and system design, and integrating it into our systems, tools, services and processes.

What is PIA and PbD

Privacy Impact Assessment (PIA)

This policy outlines the importance of assessing privacy risk in projects and situations involving change to business processes or new systems and processes. Completing a Privacy Impact Assessment (PIA) is a methodology to identify, assess and manage privacy risk.

A PIA should help you to:

- identify impacts (either positive or negative) on the privacy of the public or Police staff
- understand the privacy risks and document how those risks will be eliminated or mitigated to an acceptable level
- provide a reference point for future action and review when systems, tools, services or processes change.

Privacy by Design – a design methodology

Privacy by Design means considering privacy from the beginning of a project, making privacy part of project thinking and system design, and integrating it into our systems, tools, services and processes. The 'privacy by design' approach goes hand in hand with undertaking a PIA - privacy risks are identified early and can be designed out, or at least partly mitigated to reduce the risk and consequence if the risk eventuates.

Privacy by Design involves thinking about how Police manage personal information from collection through to its eventual destruction or disposal. The approach aligns with the allied concept of 'Security by Design'.

Privacy by Design ensures we engineer safe information handling practices into our systems, tools, services or processes for maximum and enduring impact.

Benefits of PIA and PbD

PIA - assessing privacy risk

The PIA process is designed to identify risks or potential risks to the integrity and security of personal information through changed or new business projects. A PIA may also provide assurance that a project contains limited or no risks to the business.

The PIA process assists Police to:

- comply with the Privacy Act 2020 and embed Data Protection and Use Policy (DPUP) values into how Police manage personal information
- determine the risks and effects of a change or new project, and
- evaluate options to remove or reduce potential privacy risks.

Good stewardship of personal information is enhanced by undertaking a PIA when a new project or way of handling personal information may affect privacy – either negatively or positively. PIAs (and the Privacy by Design approach) also supports our vision of having the trust and confidence of the community.

Privacy by Design has an enduring effect

Privacy by Design has an enduring effect – it means systems and processes are built to make it easier for our people to do the right thing and harder for them to make mistakes.

No individual or organisation is perfect in how it operates. In various ways, the quality of our work diminishes or decays over time. Embedding good practice into systems design helps prevent decay in our day-to-day operational practices.

The ‘by design’ approach supports privacy compliance, reducing risk for Police as it collects, stores, uses, discloses, and eventually destroys or disposes of personal information, commonly described as the ‘information lifecycle’.

Building in sound privacy practices at the start lessens or prevents privacy breaches from happening.

The Privacy by Design approach raises privacy awareness about handling of personal information across Police projects and supports early identification and resolution of privacy risks while giving increased assurance that we are meeting our Privacy Act obligations.

Completing a PIA

PIA template

The PIA template is designed to be straightforward for project teams to complete and provides an opportunity for substantive comments and explanation of risks and mitigations. Completing the PIA template ensures there is sufficient substance to enable it to be used for consultation purposes with other parties, such as the Privacy Commissioners Office.

Do I need to do a PIA?

Deciding whether completion of a PIA is necessary is assessed case-by-case basis. Make early contact with the Privacy Team in the Assurance Group about your project and they will provide advice and recommend the most suitable way forward (xxxxxxxxxxxxxxxxxx@xxxxxx.xxxx.xx).

When there is only a minor change to a system, tool, service or process it may be sufficient to simply consult with and receive advice from the Privacy Team.

If you are uncertain about the level of impact that a project will have on Police’s management of personal information, or on individuals’ reasonable expectations of privacy, a PIA will be required.

It will also be necessary to complete a PIA for large system changes or significant changes to the way Police manages personal information.

Examples of projects that may benefit from a PIA process:

- Developing an online service or creating a website or mobile app to collect personal information
- Sharing personal information with another agency, or providing access to Police systems

- Using a third-party provider to process personal information (for example, a cloud-based service)
- Introducing workplace tools that affect how personal information about staff is collected, stored, and used.

Who should carry out a PIA?

Completing a PIA does not always require a privacy specialist, Police's privacy officer or a lawyer. If a project is particularly complex or the proposed use of personal information is novel or significantly different to the status quo, engage others (either internal or external) with the requisite expertise to either lead or assist with the assessment.

It is essential Police staff involved in a project contribute to the PIA process. If an external specialist is engaged to complete the PIA it is crucial to the integrity of the assessment that our institutional knowledge is included in the development of the PIA.

When should a PIA be undertaken?

There should be early consideration of privacy issues and risks when considering any new product, service, system, or process that includes personal information. A 'by design' approach means building in privacy from the outset, so start the PIA process alongside work on your business process design work.

It is also important to understand that a PIA is a 'living document', not a one-time review. As a project changes in scope or design, update the PIA to reflect new positions and new or altered privacy risks.

Privacy by Design thinking

The principles of Privacy by Design

There are seven Privacy by Design principles:

1. Proactive not Reactive/Preventative not Remedial

Think about privacy at the beginning of your project and build privacy features into new systems, tools, services or processes.

2. Consider privacy a default setting

Privacy interests need to be at the forefront of what we do. This means being thoughtful about the personal information we collect, how we collect it, how we use and share it, how we keep it safe and how long we keep it. It also means remembering there are people behind the information we collect.

3. Privacy Embedded into Design

Privacy needs to be integral to the way Police thinks and operates – it should be embedded in our systems, tools, services and functions.

4. Full Functionality – no trade-off or loss

Our obligation to protect personal information should be an opportunity to design a better system, tool, service or process rather than a trade-off with other functionality.

5. End to end privacy protection

Protection and security of personal information should be considered at every stage of the information lifecycle, through its collection, storage, use, and eventual disposal.

6. Provide visibility and transparency

We need to be transparent with individuals about how their personal information will be used. Our communications with the public should be written in plain English and take account of other cultures and languages where possible.

7. Respect individuals' privacy rights

Design user-centric systems, tools, services or processes to support individuals' ability to exercise some level of control over their information (including an access and correction right under New Zealand privacy law).

Privacy by Design strategies

These design strategies inform a privacy-focussed design approach for ICT and digital teams:

Minimise and separate — reduce opportunities for unauthorised access to information

Hide and abstract — make it difficult for *un*authorised people to use personal information

Enforce and demonstrate — reduce the probability of unauthorised access and use

Inform and control — provide individuals with information and choices to reduce the risk to their personal information.

Further advice and assistance

For advice and assistance with PIAs, and how to bring the Privacy by Design approach to life, contact Police's Chief Privacy Officer.

Resources

PIA template Privacy Impact Assessment Template Version July 2022

Privacy: advice, guidance and tools to help government agencies improve their privacy capability and maturity. https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/

Assess project privacy risk - https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/assess-privacy-risk/assess-project-privacy-risk/

Privacy by design strategies - https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/

Last modified: 22/12/2022