AN A TO Z OF APPROVED INFORMATION SHARING AGREEMENTS (AISAs)

March 2015

Privacy Commissioner
Te Mana Matapono Matatapu

Foreword by Privacy Commissioner, John Edwards

The case for Government agencies identifying opportunities to work together to provide public services is compelling. We expect government to be efficient, to deliver services based on sound reasoning and in ways that bring the most benefit to the people they are trying to help.

Public programmes can be designed in ways that allow sensible service delivery and a collaborative approach, without intruding on individuals' rights, or exposing the agencies involved to legal risk.

The Privacy Act is, at its core, a flexible and enabling piece of legislation. However sometimes it has been perceived as getting in the way of agencies working together. Sometimes those perceptions have been true, particularly when personal information gathered for a narrowly defined purpose is to be used in a new way, by more agencies, as part of a proposed service delivery innovation.

The AISA mechanism was proposed by the Law Commission, and enacted by Parliament in February 2013 to provide an answer to the "Because of the Privacy Act" objection to innovation in service delivery.

If an agency can describe which parties are to be involved in delivering a public service, what information they need to do it, and what they are going to do with that information, they can begin to draft an AISA that will remove any questions about whether the Privacy Act is going to get in the way.

From my perspective, the model allows agencies to build in protections that allow the public to have confidence that the proposal is reasonable, proportionate and subject to adequate safeguards.

AISAs can enable the efficient, responsive and sensible provision of public services, in ways that do not sacrifice important rights, and without adding unnecessary risk of privacy breaches. We hope that this guidance document will help you to make the most of this tool.

John Edwards

Contents

Understanding AISAs 5

What is information sharing? 5

What is an AISA? 5

What does an AISA do? 5

Can private sector agencies join an AISA? 5

What does an AISA authorise? 6

Limits of an AISA 6

Does an AISA require legislation to be passed? 7

What are the advantages of an AISA? 7

No one size fits all 8

Common challenges 8

AISA legal authority checklist 9

Policy process for an AISA – what are the key steps? 10

Step 1: Is information sharing needed? 11

Is information sharing needed? 11

What personal information will be needed? 11

How will the information be used? 12

Step 2: What authority do I need? 13

Assessing legal authority 13

Does the AISA need to cover the entire process or just part of it? 13

Gap analysis 14

Is there any relevant legal authority (apart from the Privacy Act)? 14

Can I do this under the Privacy Act? 14

Other sharing options under the Privacy Act 15

Information sharing options – summary 15

Step 3: Developing an AISA 16

Engaging with the challenges of information sharing 16

Input from key people at each stage 17

Meet with the Office of the Privacy Commissioner 17

Starting a Privacy Impact Assessment 17

What we will look for in your PIA 18

Exemptions & modifications to the privacy principles to enable sharing 19

Consultation and the PIA & AISA 19

What details must be included in an AISA? 20

What else should I be thinking about when drafting the AISA? 21

Good AISA design 21

How do I deal with adverse action in the AISA? 21

Step 4: AISA approval 22

Stage 1 Getting policy approval for your AISA 22

Stage 2 Who must I consult? 22

Stage 3 Ministerial considerations – what's involved? 23

Stage 4 Order in Council (OiC) 23

Stage 5 AISA publishing 24

Stage 6 Privacy Commissioner to report on approved agreement (96P) 24

Stage 7 Formalising AISA reporting 24

Step 5: AISA review 25

Appendix: AISA contents checklist 26

Understanding AISAs

What is information sharing?

Information sharing is the disclosure of information about an identifiable individual by one agency (or a division of an agency) to another, usually for a purpose unrelated to the reason for which the information was originally collected or provided.

What is an AISA?

An AISA is a legal mechanism that authorises the sharing of information between or within agencies for the purpose of delivering public services.

What does an AISA do?

An AISA authorises agreed departures from the privacy principles (except principles 6 and 7 – access and correction rights) if there is a clear public policy justification and the privacy risks of doing so are managed appropriately.

An AISA is a means of obtaining agreement about when agencies will share personal information and in what circumstances. This can provide a high degree of certainty about the sharing of information.

Can private sector agencies join an AISA?

Non-government agencies can be involved, but the AISA has to be linked to a public service mandate and must involve a government department as the "lead agency".

What does an AISA authorise?

An AISA authorises modification or exemption to the privacy principles. In practical terms, this may change how information under the Privacy Act is:

- collected
- stored
- checked
- used
- disclosed
- exchanged

If necessary, an AISA can also authorise assigning of a unique identifier to an individual or assign a unique identifier that has been assigned by another agency.

Limits of an AISA

It is worth noting the following limitations:

- An AISA cannot enable information sharing with overseas agencies.
- An AISA does not provide an exemption from the Privacy Act – the Act continues to apply, although in a modified form. Individuals whose information is shared may raise complaints with the Privacy Commissioner.
- An AISA cannot force an agency to share information in any particular case. The mechanism enables permissive sharing rather than mandatory sharing.
- An AISA cannot override any statutory prohibition on information sharing – in that case, legislation may be needed to resolve a statutory impediment. However, an AISA can permit sharing for a different purpose or with a different agency if the information sharing provision is listed in Schedule 3 of the Privacy Act.

CHECKPOINT

Have I assessed the broader legal context in which the information sharing will occur?

Are there any relevant statutory authorities or restrictions?

IS THE INFORMATION SHARING RESTRICTED BY ANY STATUTE (OTHER THAN THE PRIVACY ACT)?

YES

IS THE STATUTORY RESTRICTION AN INFORMATION MATCHING PROVISION

No – an AISA cannot provide additional authority	Yes – an AISA can extend purpose and agency

TIP

IF YOUR PROJECT INVOLVES OVERSEAS AGENCIES WE RECOMMEND YOU SPEAK TO US AT AN EARLY STAGE TO DISCUSS ALTERNATIVE OPTIONS.

SCENARIO

The Registrar of Births Deaths and Marriages is the authoritative source of information about deceased people but few businesses and government agencies receive this information from the Registrar to maintain accurate client records. Instead, many rely on less efficient means such as word of mouth from relatives or public death notices.

The Registrar (DIA) as the lead agency could provide a service to public and private sector agencies in an administratively efficient and uniform way. New parties could be added to the agreement as required.

Scenarios are included as examples for guidance purposes only and do not represent actual policy initiatives.

Does an AISA require legislation to be passed?

The AISA process does not require legislation to authorise the information sharing arrangement, although it will require a legislative instrument – an Order in Council. As a legislative instrument, an AISA also requires a regulatory impact statement, disclosure statement and ministerial and Cabinet approvals.

In particular cases, it may be necessary to pass legislation to overcome an existing statutory restriction on information sharing, or to resolve any statutory inconsistencies.

Example – section 81A of the Tax Administration Act 1994 was added in 2013 to allow Inland Revenue to use AISAs, as an override to IR's secrecy obligation in section 81.

What are the advantages of an AISA?

An AISA can provide the following advantages:

- facilitating agency co-operation and efficiency in shared public service delivery while meeting privacy expectations
- legal authority to share where there is a lack of authority or incomplete authority
- certainty and assurance for agencies about how information will be protected, reported and deleted
- accountability and transparency for the public about information sharing arrangements
- potential to accommodate multiple parties – either as signatories to the agreement, or through a representative party
- flexibility to tailor privacy safeguards in the AISA depending on the privacy risks involved
- flexibility to make minor changes without further legislative instrument.

SCENARIO

The government wants to provide coordinated services to refugees in the Auckland region. The services include housing, income and employment support, education and language skills and health services.

An AISA between MSD, social housing providers, Immigration NZ, MoE, Auckland DHB, ESOL providers and refugee support services could enable information sharing between government and non government agencies to deliver a holistic service to refugees.

SCENARIO

There is high youth unemployment in Northland and the government wants to improve outcomes for this group.

An AISA could enable a wraparound service to be developed for school leavers. This might involve Work and Income, CYFS, Police, local schools, iwi organisations, the local employer association and other youth focused community groups. These parties could regularly meet to discuss individual cases. The AISA would describe the personal information that each party may share with each other. If the programme proved successful the AISA could be replicated in other regions.

No one size fits all

An AISA is not an "off the shelf" option – each AISA is custom-designed. The safeguards and scrutiny required will need to match the level of risk involved – the higher the risk, the stronger the safeguards and level of oversight required.

Although the AISA mechanism is flexible, the policy process can be challenging to develop for a complex sharing arrangement. However this is no different to implementing a complex proposal via primary legislation. The feasibility of using an AISA depends on a number of factors:

- The complexity of the project –
  - numbers of parties
  - range of issues and scope of the problem
  - information flows
- The legislative framework – whether there are statutory impediments or inconsistencies
- The capacity and willingness of the parties to enter into an AISA
- Organisational and operational issues
- Cost of implementation, investment and training required.

There may also be practical issues – for example, the compatibility of agency technology and whether agency systems support the proposed information sharing arrangement.

Common challenges

This guidance primarily deals with legal authority issues but noted below are the range of issues that can arise and need to be resolved in parallel to ensure that the AISA will be successful. Addressing the legal authority issues in isolation will not guarantee a successful outcome.

TIP

TRY TO KEEP THE PROJECT SCOPE MANAGEABLE BY FOCUSSING ON THE KEY GOAL.

It may be desirable to simplify, streamline or stage the project, to ensure a successful outcome:

- a series of bilateral agreements may be more manageable that one large multi-party agreement
- a representative party can be used to reduce the number of parties
- an agreement can be amended following approval to add further parties and further information flows once the initial agreement has been implemented.

TIP

WE RECOMMEND TALKING TO AGENCY OPERATIONS EXPERTS AT AN EARLY STAGE OF THE PROJECT TO IDENTIFY AND RESOLVE ANY PRACTICAL DIFFICULTIES.

COMMON CHALLENGES

WEAK PROPOSITION

- lack of clear value proposition
- inadequate business case – low cost/benefit
- ill-defined policy goal or problem definition

ORGANISATIONAL

- weak leadership
- resistant agency culture
- lack of capacity
- lack of consensus
- inconsistent information practices
- technical complexity

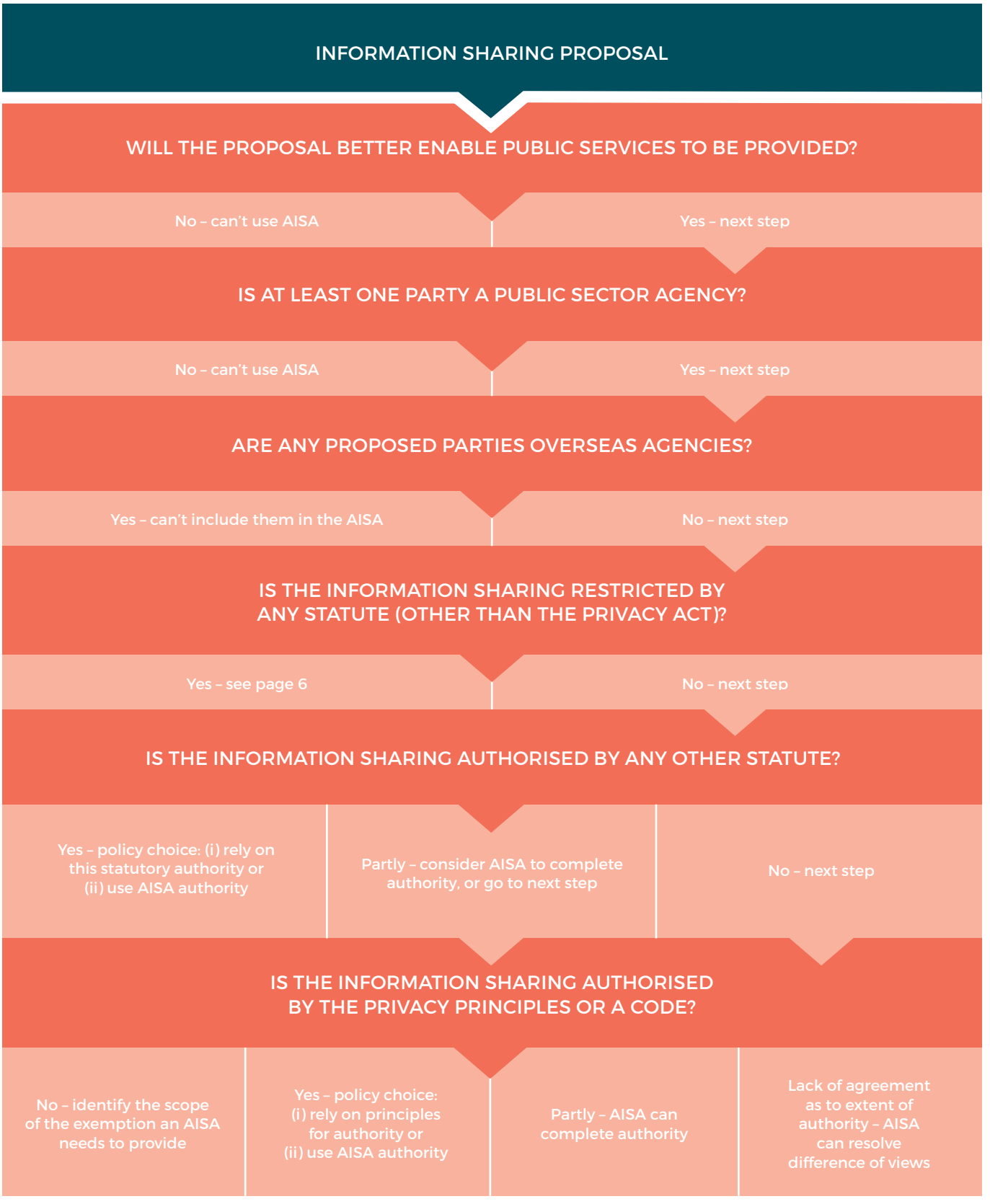
LEGAL AUTHORITY

- statutory restriction
- uncertainty
- inconsistent approach
- highly risk averse approach to legal activity

OTHER BARRIERS

- strong confidentiality values in information
- limited by international obligations

AISA legal authority checklist



Policy process for an AISA – what are the key steps?

Step 1: Is information sharing needed?

Is information sharing needed?

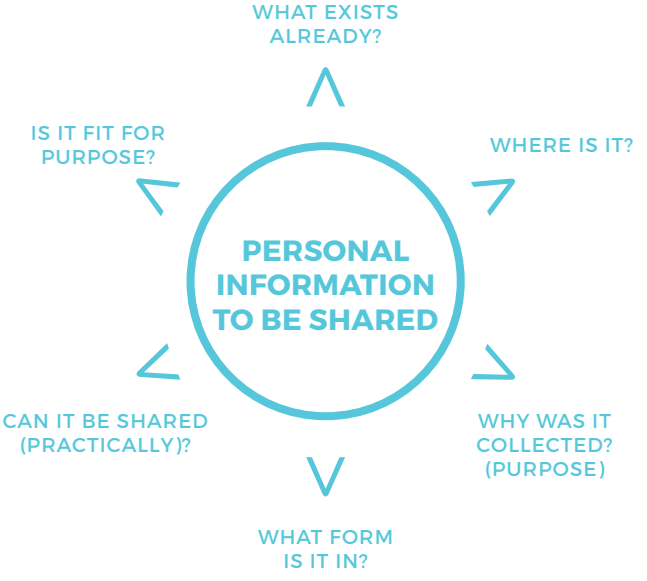
The initial step is to assess and scope the policy problem being addressed and to support the case for developing an information sharing proposal. An AISA may be one identified option, but there may be other potential options for fixing the problem without the need for information sharing. For example, the following areas should be looked at:

- data quality or attributes
- process design
- anonymising data
- collection practices
- consent practices
- notification practices
- operational practices
- information flows.

What personal information will be needed?

An important practical step is to identify the personal information needed for the project and then to assess the feasibility of getting and using it by working through the following checklist:

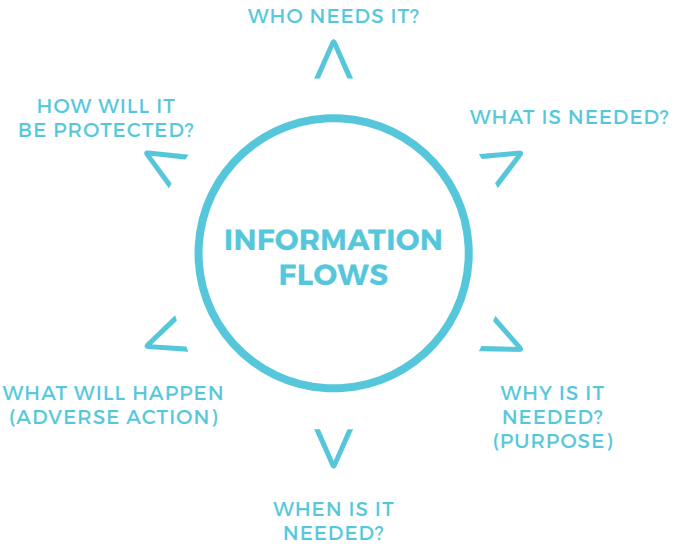
- What information exists and where is it held?
- Is the personal information already being collected:
  - by your agency?
  - by a different agency? – will that agency co-operate in principle to provide it for the project purposes?
- What purpose is the information currently being collected for? Is that purpose linked or directly related to the purpose of the proposed information sharing?
- Is the information held in a form that can be readily shared? Are the formats compatible?
- Is the information fit for the project purpose? Are improvements to the underlying data or business processes needed? Consider, for example:
  - data quality and reliability – circumstances and context of collection
  - robustness of original collection/verification processes
  - timeliness
- If the collection of additional information is necessary, consider:
  - collection channels
  - ease of collection.



How will the information be used?

Mapping the information flows will help lay the ground work for decisions about how the project should develop:

- who needs the information?
- what information do they need?
- where will they get it from?
- why (purpose)?
- when and how will they get it?
  - automatically
  - on request
  - if certain circumstances exist
  - at meetings or discussions
- what will be done with the information?
  - will it result in adverse outcomes for individuals
- how will it be protected?
  - safeguards in service delivery design.



SCENARIO

The government wants to stop youth offenders from going on to commit serious crime by implementing early intervention initiatives. To achieve this goal it has been recognised that greater information sharing is necessary.

An AISA could approve the sharing of information between members of new youth offender teams. The AISA would detail the safeguards that would be put in place to ensure information was well managed.

TIP

INVESTING IN UPFRONT ANALYSIS AND IDENTIFYING POTENTIAL ISSUES EARLY WILL SAVE TIME AS THE PROCESS UNFOLDS.

Step 2: What authority do I need?

Assessing legal authority

Information sharing to deliver public services needs to have clear legal authority. This step involves an assessment of the broader statutory context to assess the level of existing authority and to identify any legislative or other barriers.

CHECKPOINT

Would an MOU or a schedule to an existing MOU resolve any uncertainty between the project agencies about the basis for the information sharing?

Does the AISA need to cover the entire process or just part of it?

Analyse where the gaps in legal authority are in order to identify a suitable legal solution. Factors to consider:

- At each point where personal information is shared, is the sharing under an existing legal authority?
- Does any current legislation provide full or partial authority for information sharing?
- Is there any current statutory prohibition or restriction on information sharing or any statutory conflict?
- To what extent do the privacy principles provide a basis for sharing information (either fully or partially)?
- Is there uncertainty amongst partner agencies about the legal authority for the information sharing?

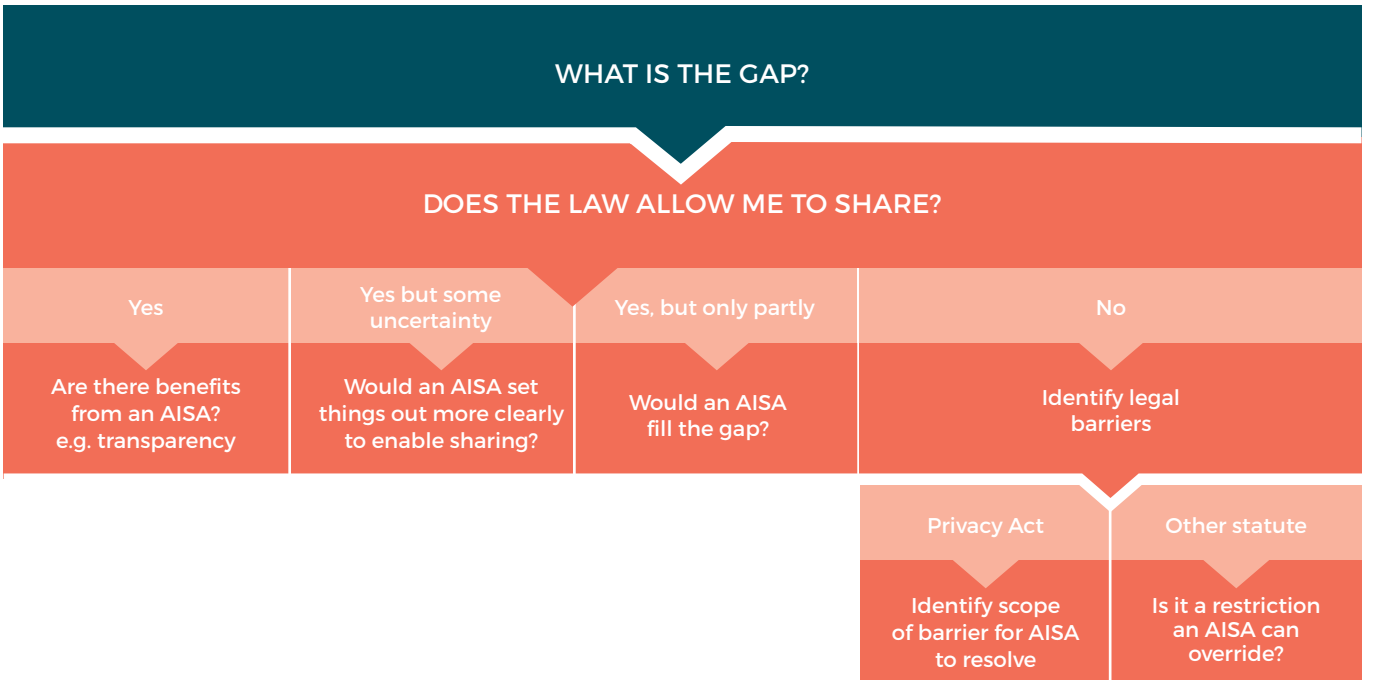
TIP

A MEMORANDUM OF UNDERSTANDING BETWEEN AGENCIES CAN HELP TO CLARIFY THE PURPOSE FOR COLLECTION, AND SUBSEQUENT DISCLOSURE FOR THAT PURPOSE.

An MOU can also clarify and record responsibilities and agreed practices for information sharing. It can be a useful tool to iron out differences of interpretation between agencies and can support a shared purpose and common goal.

However, a Memorandum of Understanding cannot legitimise disclosures that would otherwise be unauthorised because there is no legal basis to share under the Privacy Act or any other statute.

Gap analysis



Is there any relevant legal authority (apart from the Privacy Act)?

Assess the current legislation that is relevant to the agencies involved and the project context to see if there is any existing authority to share information in particular circumstances.

An example of a permissive information sharing provision is section 15 of the Children, Young Persons, and Their Families Act 1989 that allows any person who believes that any child or young person has been, or is likely to be, harmed (whether physically, emotionally, or sexually), ill-treated, abused, neglected, or deprived to report the matter to a social worker or a constable.

An example of a provision that compels information sharing is section 66 of the Children Young Persons and their Families Act 1989 that requires a government agency or statutory body to supply information to a care and protection co-ordinator, social worker, or constable for the purposes of determining whether that child or young person is in need of care or protection.

The authority contained in existing statutes may either be sufficient for the project purposes or it may only provide a partial solution.

CHECKPOINT

How far do the privacy principles provide any legal authority for some or all of the information flows?

Can I do this under the Privacy Act?

Privacy principles analysis

A privacy principles analysis helps with:

- problem identification – assessing the extent to which the proposal departs from the principles and the scope of additional authority needed
- building the policy justification for developing an AISA
- developing the PIA
- consulting OPC – to inform us about the impacts on privacy
- developing an AISA – to describe how the AISA will depart from the privacy principles
- keeping the process manageable, by simplifying an AISA to the essential departures from the privacy principles, rather than covering all information flows.

Working through the following checklist will help to identify whether the privacy principles help or hinder the implementation of the information sharing arrangement:

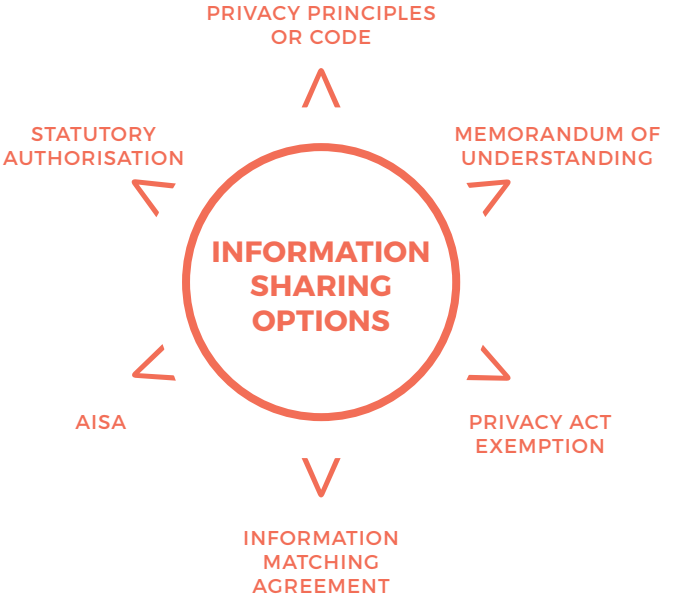
- **Can we get by without naming names?**
  Sharing suitably anonymised information is allowed under the Privacy Act.
- **Can we get consent?**
  Sharing information where the individuals have provided informed consent is permitted under the Privacy Act.
- **Is the sharing for a directly related purpose?**
  Information can be shared without consent if the sharing is for one of the purposes for which the information was obtained, or for a directly related purpose. The individual should be notified of the purpose of collection and the intended recipients of the information under a sharing arrangement.
- **Is there a serious threat?**
  Information can be shared to prevent or lessen a serious threat to anyone's life or health, or to public health or safety.
- **Is the sharing necessary for maintenance of the law?**
  Information can be shared where failure to do so would prejudice the ability of a public sector agency to uphold the law they are charged to maintain. This is not limited to law enforcement agencies and can extend to the mandate of any public sector agency.
- **Does the sharing involve bulk release of datasets?**
  The disclosure principle (privacy principle 11) can be difficult to apply to the automated bulk release of specific datasets to another agency. The principle is designed for case by case discretionary releases of personal information where the holder agency reasonably believes it to be necessary for a particular purpose such as maintenance of the law. Instead, the bulk release of data sets is usually governed by the information matching rules in the Privacy Act. An AISA is another option for this form of information sharing.

Other sharing options under the Privacy Act

The Privacy Act has a range of tools that allow information to be shared. Some of these permit the privacy principles to be overridden for a particular purpose:

- Code of Practice – e.g. the Health Information Privacy Code
- Section 54 exemption
- Information matching agreement.

Information sharing options – summary



CHECKPOINT

- Do I have a clear picture of the problem that the proposal will address?
- Do I have a clear picture of the information flows needed to deliver the proposal?
- Do I have a clear understanding about the legal barriers and options available to address them?
- Do I have the authority to proceed to develop the AISA?

TIP

THIS IS A GOOD POINT TO CONTACT OPC FOR AN INITIAL CHAT ABOUT THE PROJECT, IF YOU HAVE NOT ALREADY DONE SO.

Step 3:
Developing an AISA

Engaging with the challenges of information sharing

Key elements of the policy process

An AISA is not a short-cut policy process. The policy work involved is similar in nature and scope to a legislative proposal, but the key difference (and challenge) of the AISA process is that the policy and operational design is all front-loaded and completed ahead of the approval of the legislative instrument.

The necessary policy analysis involves:

- problem identification (gap analysis) and identification of policy options
- business case & cost/benefit analysis
- a Privacy Impact Assessment
- consultation with relevant groups and stakeholders
- consultation with the Privacy Commissioner

The AISA process also requires:

- top level approvals (Ministerial and Cabinet)
- drafting an Order in Council (PCO).

The time saving in an AISA process comes at the approval stage. The legislative instrument for an AISA is an Order in Council rather than a legislative amendment, and so it does not need to pass through the House and Select Committee process.

Any policy initiative to develop information sharing opportunities needs to identify, examine and address some common issues of inter-agency and intra-agency sharing.

The project team will also need to assess and work through any practical and cultural issues that could limit the potential for successful service delivery. Ideally, these challenges should be identified and resolved in parallel to the legal authority issues, so that an AISA can operate effectively.

SCENARIO

The delivery of social housing in rural areas could be enhanced through greater co-ordination between HNZ, IRD, MSD, emergency housing providers such as the Salvation Army, and other non-government organisations providing housing and support services.

An AISA could assist in the timely identification, eligibility and ongoing support of families that meet the criteria for social housing assistance.

Input from key people at each stage

The project will require the involvement of key people within all the agencies involved at the appropriate stages of the project. Senior management will need to be involved at critical decision-making points such as approving the business plan. The responsible Minister needs to be consulted to confirm their commitment to the scope of the information sharing.

The service design strategy and operational process details will be important to inform the policy phase of the project. That will provide essential information to guide a successful roll-out of the project.

All parties (including any representative party) to the proposed agreement should be involved in the development of the AISA. There will also need to be close collaboration with partner agencies to ensure that project goals and timelines are achieved.

Meet with the Office of the Privacy Commissioner

At this point, you'll be armed with good knowledge about your project although the finer details might not be ironed out yet. It's an ideal time to contact OPC and talk us through your proposal before you start working on the PIA and AISA.

We can talk about the privacy implications at a high level. This will give us a feel for the project in terms of how well an AISA might work versus other information sharing options. You'll be able to bring us up to speed on the proposed development timeframes. In turn we'll be able to fill you in on the AISA process and consultation requirements.

We can also talk about the role that the lead agency has in reporting on the operation of the AISA. Building in the ability to report on particular metrics at the design stage will be much easier than 'bolting on' reporting at the end of the project.

Starting a Privacy Impact Assessment

Before you start drafting your AISA we recommend that you first clearly identify and consider the privacy impacts/risks and the potential adverse outcomes for individuals associated with your proposal and how you will mitigate those impacts/risks. Identification of privacy risks at the outset enables privacy protective safeguards to be embedded into new business processes and IT system design.

What are the privacy risks?

Privacy risks from information sharing include:

- failure of security
- duplication of inaccurate information
- unanticipated uses of information

Completing a Privacy Impact Assessment (PIA) is the best way to identify privacy risks in a structured way.

TIP

WE RECOMMEND INVOLVING PRIVACY, LEGAL, OPERATIONS AND IT PEOPLE IN THE EARLY DESIGN STAGES AND AT KEY POINTS AS THE PROJECT DEVELOPS.

TIP

WE RECOMMEND USING THE PRIVACY IMPACT ASSESSMENT TOOLKIT ON OUR WEBSITE.

What we will look for in your PIA

A PIA to assess the privacy risks of an AISA will include some particular matters that we require as part of our assessment of an AISA. The following list outlines the details we expect to see included in a PIA:

- information flows (diagrams are good too)
- the information lifecycle in terms of how and when information is collected, transferred, stored, verified, used, and destroyed
- identification of privacy risks during the information lifecycle and details of the safeguards to mitigate/ manage risks to an acceptable level
- an assessment of proportionality (sensitivity/amount of information) – consider the nature of the information being shared about each individual and the purpose of the sharing. Is the significance of the project purpose proportionate to the sensitivity, amount and nature of information being shared?
- an assessment of proportionality (scale). Is the number of individuals affected by the information sharing a proportionate response? Or in other words, is the privacy cost reasonable and justified to enable the public service?
- cost/benefit analysis, including both financial costs and an assessment of privacy cost
- an assessment of the potential for an individual to incur an adverse action as a result of agencies sharing personal information about them. "Adverse action" needs to be considered in the broader context of actions that an agency can reasonably be expected to take as a result of sharing information (see How do I deal with adverse action in the AISA? below).

In addition to the details above, a PIA relating to an AISA should provide these details:

- an assessment against the criteria set out in section 96N(2) of the Privacy Act
- clear justification to support any modification to or exemptions from the privacy principles proposed to enable information sharing using the AISA.

TIP

THE PIA NEEDS TO CLEARLY IDENTIFY:

- **THE PRIVACY RISKS AND OUTCOMES FOR INDIVIDUALS, AND**
- **THE BENEFITS FOR THE INDIVIDUAL AND/OR THE AGENCIES CONCERNED.**

If the offset of benefit against the privacy risks is not compelling, it will be a much harder task getting the AISA across the line.

Exemptions & modifications to the privacy principles to enable sharing

Where information sharing is without consent of the individual, can't otherwise be done under the privacy principles and no other legal provision authorising the sharing exists, then the Order in Council that approves the AISA must grant an exemption or modify one or more privacy principles.

The following privacy principles may need an exemption or modification granted:

Principle 2: Source of personal information
If your project involves receiving personal information that another agency originally collected for another purpose (rather than collecting the information from the individual) and none of the principle 2 exceptions apply, an exemption to principle 2 will be necessary.

Principle 10: Limits on use of personal information
If your project involves personal information collected by one part of an agency for a particular purpose and sharing it with other parts of the agency for another unrelated purpose(s), and none of the principle 10 exceptions apply, an exemption to principle 10 will be necessary.

Principle 11: Limits on disclosure of personal information
If your project involves a reciprocal exchange of information between agencies; one or more agencies providing information to another agency; or several agencies pooling information and making it available to each other (like a common database), and none of the principle 11 exceptions apply, an exemption to principle 11 will be necessary.

An exemption cannot be granted to modify principle 6 or 7 (access and correction rights).

Consultation and the PIA & AISA

The Privacy Act requires that affected parties are consulted (and submissions invited) about the proposed AISA. It may be a useful exercise to distribute and seek comment on the draft PIA at the same time. Consulting with organisations that represent affected people during the development of the PIA can help identify additional downstream privacy impacts.

The PIA is a key document necessary for consultation with OPC. We will review the PIA alongside the draft AISA. Privacy risks identified in the PIA should be mitigated by appropriate safeguards within the AISA.

We expect the first draft of the PIA and AISA to be quite well developed. We will provide you with prompt but substantive comments where necessary on the:

- identification and mitigation of privacy risks
- information handling design
- privacy analysis and justifications
- legal analysis and justifications
- cost/benefit analysis
- content of the AISA.

CHECKPOINT

Have I engaged with IT, business/operations on process design?

What details must be included in an AISA?

The Privacy Act (section 96I) sets out what detail must be included in the AISA. The key components are:

- **A purpose statement**
  This needs to provide in reasonable detail the objectives or outcomes that the agreement seeks to achieve.
- **The parties to the agreement**
  The parties to the agreement may be government agencies or private sector agencies. A 'representative party' can act on behalf of a class of agency (listed in the Schedule of Parties), either by name or by sufficient description to identify who is included. If you can clearly describe a group of agencies by class, the AISA does not have to list them all by name.

  An example of a representative party is The Royal New Zealand College of General Practitioners. In this case the Schedule of Parties could specify "registered general practitioners" as the class of agency represented.

  A lead agency (must be a government department) must also be named.
- **An overview of operational processes**
  Include details about information flows, how information will be used, and what actions are to be taken by which parties
- **Details of safeguards to the privacy of individuals and statements of how any privacy interferences are minimised**
  Include details about how information will be kept secure throughout the information lifecycle. For instance, safeguards to protect information in transit, verification of information before it is acted upon, protocols for contacting individuals, storage and destruction of information.
- **Details of any exemption or modification of any privacy principles or code**
  Details about exemptions to privacy principle 2 (collection), and 11 (disclosure) will be necessary in most cases.
- **A detailed description of the personal information or type of personal information to be shared and how each party may use that information**
  For example, first names, surname, date of birth, home address, employer name, passport number, email address, financial transaction information. Make sure that the wording in your agreement allows you to fulfil the policy objectives.
- **Details of any adverse action that any party is likely to take and the procedure that will be followed if notice of adverse action is not provided**
  See the section below on "How do I deal with adverse action in the AISA?"
- **Details about complaint handling**
  Mention any special circumstances relating to the handling of complaints. Include a simple statement saying that the parties will provide appropriate assistance to any individual to determine where a complaint should be lodged.
- **Details of where a copy of the agreement can be accessed**

What else should I be thinking about when drafting the AISA?

The following 'privacy protective' measures should guide your thinking:

- share the minimum relevant personal information necessary about each individual with the minimum number of agencies (and staff within each agency) to deliver the public service
- only share information about individuals that will qualify for the public service
- design safeguards that adequately address the privacy risks identified in the PIA process
- restrict the allowable purpose(s) that information can be used for within the agreement (restrict secondary use)
- build in a periodic review period to verify the effectiveness of the AISA against the stated purpose.

Good AISA design

How do I deal with adverse action in the AISA?

Working out what adverse action could eventuate should be considered in the broader context of actions that an agency can expect to take as a result of sharing information. Think about the purpose of the sharing and what the potential outcomes or downstream consequences will be rather than a narrow view about the initial exchange of information.

Some examples of adverse action include:

- disclosure of sensitive information to a family member or support worker
- investigation, arrest or prosecution
- enforcement action or debt recovery
- withdrawal of services
- reduction or cancellation of entitlements.

Unless the AISA or Privacy Commissioner authorises a reduced notice period or dispenses with giving notice, a written notice must be sent to an individual before adverse action is taken against them if the action is based on information shared under the agreement.

Where an agency wishes to dispense with sending a notice, the Order in Council (and AISA) must state the procedure that will be followed before an adverse action is taken. Those procedures need to be designed to protect individuals from inappropriate actions against them, for instance to protect people against being wrongly targeted due to mistaken identity.

In some situations, sending an adverse action notice may undermine the purpose of the sharing arrangement. In other situations, having alternative processes and safeguards will be a more privacy protective and cost effective way of delivering the public service.

CHECKPOINT

- **Have I engaged with OPC?**
- **Have I completed a draft PIA and AISA?**
- **Has the Minister agreed to proceed with public consultation?**

Step 4:
AISA approval

An AISA is approved by Order in Council on the recommendation to Cabinet by the Minister responsible for the 'lead agency' in the agreement. Before making that recommendation the Minister must consider submissions received as part of the AISA consultation phase, and the matters in section 96N of the Privacy Act.

Stage 1
Getting policy approval for your AISA

Because the Order in Council (OiC) implementing an AISA is a legislative instrument, the policy decisions underpinning an AISA should be considered by a Cabinet Committee **prior** to the Minister making their recommendation to approve the AISA at Executive Council. This process accords with paragraph 7.86 of the Cabinet Manual.

The policy approvals for an AISA should cover the high-level description/approval of the process and information flows, any overrides of information privacy principles required and any formal exceptions required (e.g. to adverse action rules). It is not expected that the policy approval will cover all aspects of the AISA. Some of the finer details of the agreement will not be worked out until after matters raised during the consultation phase have been addressed.

Getting Cabinet Committee approval

There are two obvious scenarios for how an agency might choose to seek Cabinet approval of the policy decisions underpinning an AISA:

1. **Ministerial approval to proceed > draft AISA and consult > Cabinet committee paper approving policy > draft OiC and LEG paper.**
   This is the best practice approach from our perspective because it allows room for the consultation process to inform the policy development, prior to seeking Cabinet approvals.
2. **Cabinet approval to proceed and policy decisions > draft AISA and consult > report on consultation, draft OiC and LEG paper.**

An agency will need to be confident that the AISA meets Ministerial statutory criteria under section 96N(2) before seeking policy approvals (this applies to both scenarios).

In each of the above scenarios, Cabinet Office rules require agencies to consult the Privacy Commissioner on the policy decisions put forward, even if the statutory consultation with affected parties is to be done after seeking policy approvals.

Stage 2
Who must I consult?

Before an AISA is finalised, the agencies involved in the agreement must consult and invite submissions about the agreement from the Privacy Commissioner and organisations that represent the interests of the classes of individuals whose personal information will be shared.

Representative industry groups, umbrella organisations and community groups that can provide meaningful feedback on the likely impact of the AISA are examples of organisations to consult. The key agencies involved in the AISA will need to determine the nature of the consultation (consultation length, number of groups consulted, and type of outreach). The Privacy Commissioner can comment on the consultation process that the agencies carried out as part of his report on an approved agreement.

A copy of each submission must be provided to the responsible Minister (the Minister in charge of the lead agency) for them to consider before making a recommendation about the making of an Order in Council.

TIP

GETTING FEEDBACK FROM AFFECTED INDIVIDUALS EARLY IN THE POLICY DEVELOPMENT PHASE IS MORE LIKELY TO RESULT IN A BETTER POLICY OUTCOME.

OPC consultation

We expect the first draft of the PIA and AISA to be quite well developed. Overall, we expect to see no more than three draft versions of your PIA/AISA during the consultation phase.

We will usually provide you with comments on each draft PIA or AISA promptly. Particularly complex and involved sharing proposals may take us longer to respond to.

Once the final draft version of the PIA and AISA are complete we will usually provide a written submission (section 96O) to the lead agency within 10 days.

Our role is to assess the privacy implications of the proposed agreement. Our practice is to structure our submission by responding to the criteria in section 96N(2) of the Act.

Our submission must be provided to the responsible Minister.

CHECKPOINT

Having reviewed the submissions:

Are any changes needed to the project?

Does the Minister need to be informed of any issues?

SCENARIO

The elderly are an at risk group in the community subject to increasing levels of neglect and abuse. A lack of information sharing is seen as a barrier to effective service delivery.

An AISA could approve sharing between support agencies such as Age Concern, iwi organisations, Pacific community organisations, the Royal NZ College of General Practitioners (as a representative party for GPs) and a lead government agency such as MSD. Consultation might include Greypower, NZ Law Society, Public Trust, Māori Women's Welfare League and Presbyterian Support Services.

Stage 3
Ministerial considerations – what's involved?

The lead agency for the proposed AISA must brief their Minister so that he or she can be satisfied that the criteria set out in section 96N(2) of the Act have been met before recommending making an Order in Council to the LEG committee.

That briefing will include providing the Minister with:

- a copy of the submission received from the Privacy Commissioner and others
- documents that explain the AISA design and how the AISA satisfies the information sharing requirements in the Privacy Act.

Stage 4
Order in Council (OiC)

What does the OiC need to include?

Section 96K sets out what must be included. In summary, the OiC must include details of:

- exemptions or modifications to the privacy principles
- the public service intended to be facilitated
- the personal information or type of information to be shared
- the parties to the agreement, including designating the lead agency
- what personal information can be shared by each party with each of the other parties
- how each party may use the personal information it receives
- any adverse action anticipated by any party to the agreement
- the procedure each party will follow before taking adverse action if no notice is provided to individuals
- how to access a copy of the agreement.

When does the OiC come into force?

The OiC comes into force on the date specified in the OiC, and usually must not come into force until at least 28 days after it has been notified in the New Zealand Gazette.

TIP

ALLOW A ONE-WEEK TURN AROUND FOR COMMENTS FROM OPC ON DRAFT PIA/AISA

ALLOW A MINIMUM TWO MONTH PERIOD FOR ALL CONSULTATION FROM THE CREATION OF FIRST DRAFT DOCUMENTS. MULTI PARTY AGREEMENTS ARE LIKELY TO TAKE LONGER.

Stage 5
AISA publishing

Once the agreement has been approved by OiC, the lead agency is responsible for publishing the AISA on their website, or on another public sector agency website the lead agency Minister has designated.

Stage 6
Privacy Commissioner to report on approved agreement (96P)

Once the AISA has been approved by Order in Council the Privacy Commissioner will provide a report (under section 96P) on the agreement to the lead agency Minister.

The report will repeat much of the same information provided in our submission under 96O to the lead agency prior to the agreement being approved. In addition, the report may include comments on the adequacy of the consultation process.

Our 96P report will be published on the OPC website (after consulting with the lead agency Minister) unless there are good reasons not to. Publishing the report is an important public transparency exercise enabling the public to review the reasoning and position taken by the Privacy Commissioner on the agreement.

Stage 7
Formalising AISA reporting

The lead agency is responsible for reporting on the operation of the AISA in their annual report. The details of what must be reported, and how often, is specified by the Commissioner in a reporting notice.

Regulations (Privacy Amendment Regulations 2013) govern what matters OPC can request the lead agency to report on. OPC must consider the cost of reporting, the likely public interest and the privacy impacts linked with the agreement when designing an appropriate reporting regime. The reporting regime is intended to provide public transparency on the scale, costs, benefits and assurance aspects of the AISA.

In practice, the process of deciding what reporting will be required is done in close discussion between OPC and the lead agency. It's a good idea to talk with us early about what the likely reporting will entail rather than waiting until the AISA has been approved and business processes are finalised.

Agencies regularly complete process audits or other assurance checks on their business processes. Reporting on audit and assurance activity is a key mechanism to retain public trust in an AISA. OPC actively monitors compliance with this requirement.

Examples of reporting metrics are:

Scale

- Number of records received
- Number of records successfully matched
- Number of adverse actions completed

Costs

- Estimated on-going operating cost

Benefits

- Number of successful contacts
- Estimated number and value of payments received/given
- Percentage of those contacted who have moved to compliant status

Complaints

- Number of complaints received by the Privacy Commissioner

Operational difficulties

- Details of significant error events

Assurance

- Where an audit or other assurance process has been undertaken, a summary of the results of that audit or assurance process.

Step 5:
AISA review

The Commissioner can review the operation of an AISA after the OiC has been in force for 12 months.

Where the review uncovers matters of concern, for example, if there is a failure to deliver the public service in an effective manner, or unforeseen privacy impacts are occurring, the Commissioner may report those findings to the lead agency Minister. The Minister must table the Commissioner's report in the House and set out the Government's response to that report.

Appendix: AISA contents checklist

REQUIRED COMPONENTS (SECTION 96I OF THE PRIVACY ACT)
1. Specify the purpose of the information sharing agreement. This must clearly define and express the objective(s) of the AISA.
2. State the public service(s) which the agreement is intended to enable.
3. Specify in detail the personal information or type of personal information to be shared.
4. Set out the parties (or classes of parties) to the agreement and designate one party as the lead agency.
5. If applicable, name any Representative Party to the agreement, and include in a schedule the class of agencies or name the individual agencies represented.
6. For each party to the agreement describe: • the information or type of information that the party may share with each of the other parties • how the party may use the personal information • the adverse actions that each party can reasonably be expected to take • the procedure that each party will follow before taking adverse action where a notice of adverse action is not provided.
7. State the exemptions and/or modifications to the information privacy principles.
8. Provide an overview of the operational details about how information will be shared.
9. Specify the safeguards that will be used to protect personal information and minimise privacy risks as a result of sharing under the agreement. Set out the safeguards that protect privacy through the information life cycle covering: • transfers of information electronically or by manual means • verifying/confirming information/ identity • secure storage and access controls • retention and deletion process/policy • staff training/policies • assurance (audit) practices.
10. Specify the public sector agency responsible for managing privacy complaints where a private sector agency cannot be held to account for those complaints.
11. Assistance statement – commit to providing assistance to the Privacy Commissioner or an individual that wishes to make a complaint to determine the agency against which the complaint should be made.
12. State how the agreement can be accessed.

USEFUL ADDITIONAL INFORMATION

1. Fees and charges payable under the agreement.

2. Defined terms section to explain technical terms and acronyms.

3. Agency contact details.

4. Dispute resolution.