Privacy Commissioner
Te Mana Matapono Matatapu

Information Matching Bulletin

News from the Office of the Privacy Commissioner – June 2013

In this edition

IR contact student loan borrowers using Customs border data

Inland Revenue recently started making contact with student loan borrowers in serious default through a new information matching programme with Customs.

The new programme uses the same processes Inland Revenue has to contact people in default of their child support obligations. Inland Revenue maintain an electronic 'alerts' file of all student loan borrowers of interest within the Customs environment. When borrowers on the alerts file crosses the border, Customs staff will be notified to copy details from arrival or departure cards and send them to Inland Revenue.

Changes to the Customs and Excise Act 1996 (section 280H) authorising the programme were assented in March 2013.

Identity Verification Service goes live

The Identity Verification Service (IVS) went live in April 2013. The IVS enables people to verify their identity to participating government agencies online using an Electronic Identity Credential (EIC). The EIC is more commonly known as an igovt ID.

In order to verify identity information provided by a person applying for an igovt ID (and to keep the information about the igovt ID accurate and up to date), an information matching programme is used to verify the information collected by the IVS with the following agencies that hold identity information:

- The Registrar General Births, Deaths and Marriages
- Department of Internal Affairs Passport Office
- Department of Internal Affairs Citizenship Office
- Ministry of Business, Innovation and Employment, Immigration.

The Electronic Identity Verification Act 2012 (Section 39) authorising the programme was assented in December 2012.

MSD to enforce Justice warrants to arrest through benefit system sanctions

From July 2013, MSD will help enforce Justice Warrants to Arrest (WTA) through benefit system sanctions using a new information matching programme with the Ministry of Justice.

The new programme will target beneficiaries in receipt of current benefits who are defendants in criminal proceedings. Beneficiaries with alleged low-level offending, for example non-payment of fines, will not usually be subject to this programme as most fines are civil and not criminal offences.

Justice will supply MSD with information about people with relevant WTAs that have remained unresolved for 28 days. For matched clients, MSD will notify clients that they have 10 days to resolve their WTA, otherwise benefit payments will be suspended (or reduced if the client has children in their care) until the WTA has been resolved by the client.

The Social Security (Benefit Categories and Work Focus) Amendment Act authorising the programme was assented in April 2013.

IR use birth records for new child support match

In January 2013, IR started matching against birth data provided by the Registrar-General to enable IR to establish the tax file numbers of parties within the child support scheme, in particular qualifying and dependant children. The introduction of reforms to the child support scheme effective 1 April 2014 requires tax file numbers to be established for all children currently within the scheme.

The disclosure of births information for this programme is authorised by S.78A (schedule 1A) of the Births, Deaths, Marriages and Relationships Registration Act 1995.

MSD use overseas born name change records for new match

In October 2012, MSD started receiving data from the Name Change Register administered by the Registrar-General. The Name Change Register contains information about people born overseas whose name change has been registered in New Zealand. MSD use the information to verify MSD client eligibility or continuing eligibility for benefits or allowances.

The disclosure of information for this programme is authorised by S.78A (schedule 1A) of the Births, Deaths, Marriages and Relationships Registration Act 1995.

Approved Information Sharing Agreements (AISAs) – a brief outline

Colin Trotter

Purpose of AISAs

On 27 February 2013, new Part 9A ("information sharing") was inserted into the Privacy Act. Part 9A provides a framework for the authorisation and oversight of AISAs that enable personal information to be shared between (or within) organisations for the purpose of delivering public services.

Consultation and process basics

AISAs are approved by Order in Council on the recommendation of the Minister responsible for the AISA's 'lead' agency. AISAs have the status of regulations and are subject to review by the Regulations Review Committee.

Before the Minister can recommend approval of an AISA, the Minister must invite and consider submissions from the Privacy Commissioner and other representative parties, and be satisfied that:

- the AISA will facilitate the delivery of public services
- the type and quantity of personal information shared is only that which is necessary
- the AISA does not unduly impact on individual privacy and adequate privacy safeguards are in place
- the benefits of sharing information are likely to outweigh financial and other costs
- any potential legislative conflicts have been resolved.

AISAs can modify or override the Privacy Act information privacy principles or codes of practice. However, AISAs cannot modify or override an individuals right to access and correct their personal information (IPP6 &7).

No person or organisation can be compelled to be a party to an AISA. An AISA authorises but cannot compel information sharing.

Where Acts of Parliament prohibit information sharing, AISAs cannot override them.

Parties

One party to an AISA must be designated the lead agency, and it must be a government department. For the purpose of AISAs, government department includes the Police and New Zealand Transport Agency. Any person or organisation can be a party to an AISA, including any in the private sector, but not a person or organisation outside NZ.

An organisation that represents the interests of members of a profession (such as doctors) or types of institutions (such as schools) can be party to an AISA. Such parties represent what are known as a “class of agencies”.

AISA content

The Privacy Act prescribes what content must be included in an agreement. For example, the AISA’s purpose, what privacy safeguards are in place, and what information will be shared and how must be included.

Role of the Privacy Commissioner

Before approval: The Privacy Commissioner must be consulted and may make a submission on the proposed AISA. Any submission must be provided to the responsible Minister.

After approval: The Privacy Commissioner may prepare and publish a report about the AISA or the consultation process. The Privacy Commissioner may also conduct a review of the operation of the AISA and report to the Minister responsible for the AISA’s lead agency.

Reporting by lead agency

The lead agency must report details (as directed by the Privacy Commissioner) about the operation of the AISA in their annual report.

A copy of the AISA must be accessible online, free of charge.

Ministry of Justice Flow Chart

The Ministry of Justice has created a useful flow chart of the AISA authorisation process (see below).

1. IDENTIFY PROBLEM & PARTIES

Determine public services to be facilitated & parties

-One party must be a department (or the Police or NZTA)

-One party must be designated the "lead agency", and must be a department (or the Police or NZTA)

-Parties can be non- public sector (eg, NGOs)

2. MEET & TALK

Parties meet to discuss and agree on an information sharing agreement

-Identify and resolve potential privacy risks

- A Privacy Impact Assessment may be appropriate

-Contact Office of the Privacy Commissioner (OPC) to find out what their expectations are & expertise they can offer

3. AGREE

Parties agree on an information sharing agreement

Agreement includes:

-The lead agency & parties

-Information to be shared

-How personal information may be used

- How information will be protected

4. CONSULT

The parties consult with:

-The Privacy Commissioner

-Any person or organisation that represents the interests of the class of individuals whose personal information will be shared

-Relevant others

5. MINISTER CONSIDERS & RECOMMENDS

The lead agency's Minister has regard to (inter alia):

-Any submissions from the consultation (includes the Privacy Commissioner's)

-Whether the Agreement unreasonably impinges on privacy

-That benefits outweigh costs

6. APPROVED BY ORDER IN COUNCIL

Made on the recommendation of the Minister

The Order in Council may make an exception or modify information privacy principles (but not IPPs 6 or 7 that concern an individual's right to access and correct their personal information)

7. PUBLISH & REVIEW

The Agreement is published and made publically available

- Lead agency regularly publishes report on the operation of the agreement

- The Privacy Commissioner *may* publish a report on the agreement (but not required)

- From 12 months after approval, the Privacy Commissioner may at any time conduct a review of the operation of the Agreement

8. AMEND AGREEMENT

The parties may amend an Agreement by repeating the agreement process stages 3-6

- No need to repeat stages 3-6 if changes have no privacy implications

-The most up-to-date Agreement must be available on the internet

Information matching workshops

Are you planning on running a new information matching programme, or new to working with a current programme? If so, you'll need to know how to evaluate the privacy implications involved. We call these information matching privacy impact assessments or IMPIAs. To find out more and to get some practical background knowledge on the Privacy Act, enrol in one of our half-day workshops.

The cost is $180 (includes GST) per person. Agency dedicated workshops are negotiated on a case by case basis.

Our next workshop is tentatively scheduled for late 2013, but is dependent on having enough participants registered. To register your interest in attending this workshop, contact Sharon Newton on (04) 474-7590 or by email to sharon.newton@privacy.org.nz.

Publications

To find out more about information matching, check out some of our other resources and publications at http://privacy.org.nz/data-matching-introduction/

Contacts

Wellington
4th Floor, 109-111 Featherston Street
PO Box 10-094
Wellington, New Zealand
Telephone: 64-4-474 7590

Simon Rae
Team Leader, Policy and Technology
Direct Line: 64-4-494 7082

Neil Sanson
Data Matching Compliance Adviser
Direct Line: 64-4-474 7592

Colin Trotter
Senior Adviser, Data Matching Compliance
Direct Line: 64-4-494 7087

You can contact us by email. Our standard email format is first name.surname@privacy.org.nz