Office of the
Saskatchewan Information
and Privacy Commissioner

Data Matching

Introduction

These days, the media has many stories about data analytics. It is praised as a tool that will bring new insights and thus, solutions. In the paper world such analysis would have been done by methodically going through a large number of filled out forms or files. With the advent of electronic databases, the ability to quickly process the data electronically is a great time saver. Results can be obtained so quickly. Many government ministries or crown corporations or health trustees have multiple databases and researchers have and will realize that they could perform so much more if they could take information from one database and compare it to information from another database. The idea even becomes more tempting and rewarding if one organization can combine data in one of its databases with information in another organization's database. When you contemplate information from various databases, you are in fact talking about data matching.

Traditional access and privacy laws are inadequate to protect citizens' information rights. These laws contemplate information flowing in distinct transactions between separate and distinct public bodies. Data matching, on the other hand, involves information flows that are not distinct. It is the aggregation, manipulation, and analysis of large and complex data sets. If not designed well, the result may be that individuals, or groups of people, may be unfairly treated.

Definitions

(a) **"big data"** - the term 'big data' is used for a lot of different things, and it can be difficult to pin down one single definition. In general, when the term 'big data' is used, it is referring to data collections that cannot be easily managed or understood using traditional means because of the size, irregularity or complexity of the data. (Ontario IPC Fact Sheet at https://www.ipc.on.ca/wp-content/uploads/2017/01/fact-sheet-big-data-with-links.pdf)

(b) **"big data analytics"** - refers to the various methods and tools used to generate insights from big data. Algorithms can be applied to large collections of data to identify patterns and connections, derive rules to automate decision-making and even predict the results of a course of action, including a person's behaviour.

(c) **"data"** means any facts, statistics, instructions, concepts or other information in a form that is capable of being communicated, analyzed or processed (whether by an individual or by a computer or other automated means); (New South Wales)

(d) **"data analytics work"** means the examination and analysis of data for the purpose of drawing conclusions about that data (including, for example, conclusions about the efficacy of government policies, program management or service planning and delivery by government sector agencies); (New South Wales)

(e) **"data linking"** means the linking or combining of personal information in one database with personal information in one or more other databases if the purpose of the linking or combining is different

i) the purpose for which the information in each database was originally obtained or compiled, and

ii) every purpose that is consistence with each purpose referred to in paragraph (a). (BC IPC)

(f) **"data mining"** means the process of discovering interesting patterns and knowledge from large amounts of data;

(g) **"data matching"** means the creation of individually identifying information by combining individually identifying or non-identifying information or from two or more electronic databases; (Alberta, similar to BC's data linking)

(h) **"predictive analytics"** means the branch of data mining concerned with forecasting probabilities; (Computerworld article business-intelligence/predictive-analytics)

Benefits of Data Matching

Government institutions and trustees do have large and complex data sets. Data matching is a practical method of aggregating and analyzing these large data sets for the purpose of gaining insights into patterns and trends that may otherwise go undetected. Such insights may support decision-making, policy development, system planning, resource allocation, and performance monitoring. Further, data matching may assist in detecting fraud, waste, or abuse.

Risks of Data Matching

Data matching is a highly invasive activity that often leads to inaccurate information about individuals. In the document *Guidance Note for Departments Seeking Legislative Provision for Information Matching*, the Office of the Privacy Commissioner of New Zealand have said that the benefits of data matching are often exaggerated and the costs underestimated.

In a recent speech by the Ontario Information and Privacy Commissioner (ON IPC), he warns that big data, or data matching programs that are not designed properly can result in uses of personal information that may be unexpected, invasive and discriminatory. He cites the following as privacy risks of data matching. Failure in design may result from:

- the use of poorly selected sets that have incomplete information, contains incorrect or outdated information, or disproportionately represent certain populations,

- the incorporation of implicit or explicit biases, and
- the lack of knowledge or transparency regarding the inner logic of the system.

Further, the ON IPC cautions us against the generation of pseudo-scientific insights that assume correlation equals causation.

With poor design, data matching can unfairly place the onus upon individuals to undertake a potentially expensive and time-consuming process of proving the data match is incorrect. For example, the US Department of Health, Education and Welfare (US HEW) data matched its list of welfare recipients with a list of its own employees. This data matching resulted in 33,000 matches. After a year of investigation, US HEW determined there were really only 638 cases of possible fraud. Only 55 of these cases were actually taken to court. (Information technology and dataveillance by Roger A. Clarke. Communications of the Association for Computing Machinery, Inc. May 1988. Page 498)

Further, if the resulting information from data matching is erroneous, then government institutions, local authorities, and health trustees may be basing their analysis of policies, programs and services on erroneous information. This may have a significant impact upon the programs and services individuals rely on.

Inadequacy of Current Legislation

Data matching presents privacy challenges that cannot be adequately addressed by current access and privacy laws in Saskatchewan. For example, *The Freedom of Information and Protection of Privacy Act* (FOIP) requires that government institutions collect personal information directly from an individual. However, data matching relies on the indirect collection of personal information. Another example is that FOIP requires that government institutions use personal information for the purpose for which it was collected. However, data matching is using personal information for purposes other than for which it was collected without the consent of the data subject.

Further, under FOIP, individuals have the right to access their own personal information. This is so that individuals can hold government institutions accountable for decisions that affect them. Unfortunately, as cited by the ON IPC, the lack of knowledge or transparency regarding the inner logic of data matching programs, or the lack of algorithmic transparency, prevents individuals from understanding how decisions are being made about them.

At times, individuals have little choice but to exchange some of their personal information for public services. Saskatchewan's access and privacy laws were created in a time where data matching was not a prevalent activity. My office recommends the creation of a stand-alone statute that regulates data matching activities by government institutions, local authorities and health trustees. Such legislation will ensure that data matching activities are done in an open and transparent manner while the privacy rights of individuals remain intact.

Legislative Review

My office reviewed data matching legislation from other jurisdictions including British Columbia, Alberta, New South Wales (Australia), New Zealand, and the European Union.

British Columbia

In British Columbia, data matching is referred to as "data linking". British Columbia's *Freedom of Information and Protection of Privacy Act* (BC-FIPPA) sets out requirements for public bodies when they are undertaking a data-linking initiative. Some of these requirements include notifying the Commissioner at the early stage of developing a data-linking initiative, completing a privacy impact assessment, and having the Commissioner review and comment on the privacy impact assessment. An extract of relevant provisions can be found in Schedule A to this report and the entire Act can be found at http://www.bclaws.ca/civix/document/id/consol26/consol26/96165_00.

Alberta

Similar to British Columbia's FIPPA, Alberta's *Health Information Act* (AB-HIA) requires custodians to complete a privacy impact assessment before performing data matching. The privacy impact assessment must be submitted to the Commissioner for review and comment.
An extract of relevant provisions can be found in Schedule B to this report and the entire Act can be found at http://www.qp.alberta.ca/documents/Acts/H05.pdf

New South Wales (Australia)

New South Wales' *Data Sharing (Government Sector) Act 2015* (NSW-DSGSA) facilitates the sharing of data by government sector agencies to a centralized department called the Data Analytics Centre. Data is to be used to support policy making, program management and service planning and delivery. An extract of relevant provisions can be found in Schedule C to this report and the entire Act can be found at http://www5.austlii.edu.au/au/legis/nsw/num_act/dssa2015n60336.pdf

New Zealand

In New Zealand, data matching is referred to as "information matching". Sections 97 to 109 and Schedule 4 of New Zealand's *Privacy Act 1993* (NZ-PA) deals with information matching for the purpose of detecting discrepancies in information about an individual, which may result in action that adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual. An extract of relevant provisions can be found in Schedule D to this report and the entire Act can be found at http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

European Union

The European Union's *General Data Protection Regulation* (EU-GDPR) regulates the processing of individuals' personal information. The *General Data Protection Regulation* features provisions that ensure that individuals are notified of the logic used behind automatic decision-making. This ensures that individuals are empowered to know how decisions are made that may affect them. Since data matching can result in erroneous information, individuals can challenge any information resulting from data matching that adversely affect their rights. An extract of relevant provisions can be found in

Schedule E to this report and the entire Act can be found at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Comparison of Legislation

Overall my office considered NZ-PA was the best model as it featured provisions that ensure individuals' rights and requiring public bodies to be accountable for their data matching activities. Below are some important themes addressed by NZ-PA:

Accountability: From time to time, public bodies engaged in data matching activities must report to the Commissioner about the data matching activities, including the actual costs and benefits of the data matching activities.

Timely destruction of information: Information that is used for data matching but does not reveal any discrepancy about an individual must be destroyed. Information that is used for data matching but reveals a discrepancy must be destroyed as soon as practicable after the information is no longer needed to take action against any individual.

Accuracy of information: Since errors occur in data matching programs, Schedule 4 of the *Privacy Act 1993* requires that public bodies establish reasonable procedures for confirming the validity of information about individuals before the public bodies rely on such information to take action against an individual.

Individuals' rights: Schedule 4 of the *Privacy Act 1993* requires that public bodies take all reasonable steps to ensure individuals affected by the data matching program are notified of the program. Further, individuals are notified if a public body will be taking action that may adversely affect them as a result of a data matching program, including the particulars of the data match. Then, individuals are given an opportunity to show why action should not be taken.

Oversight: Written agreements between public bodies must be forwarded to the Commissioner. Also, the Commissioner must assess and report on data matching program's compliance with sections 99 to 103 and schedule 4 of the *Privacy Act 1993*.

Both BC-FIPPA and AB-HIA were very helpful in that they require privacy impact assessments to be completed and submitted to the Commissioner for review and comment prior to performing data matching.

The EU-GDPR is comprehensive and features provisions that requires that the organization responsible for data matching to notify individuals, whose information is being used, of the logic of any automated decision-making, as well as the significance and the envisaged consequences of the data matching for the individual.

The focus of the NSW-DSGSA is to facilitate the flow of government data to a centralized Data Analytics Centre for the purpose of supporting "government policy making, program management and service planning and delivery". Some drawbacks of New South Wales' legislation are that:

- it does not require public bodies to notify individuals that their information is being collected, used, and disclosed for data analytics;
- it also does not require public bodies to ensure accuracy or completeness of the information;
- it also requires public bodies to destroy information after a certain time period; and
- one could imagine that if errors existed within the information used for data matching, and there was no need to ensure accuracy or completeness of the information, then errors would be perpetuated endlessly.

As a result, my office felt that NZ-PA provided the best starting point for developing proposals for legislation in Saskatchewan and then to take certain provisions from Alberta and the European Union. Finally, after borrowing from these three jurisdictions, it is also necessary to adapt legislation to ensure that it would work effectively in Saskatchewan.

The Saskatchewan Situation

In Saskatchewan government institutions such as ministries and crown corporations administer programs that benefit citizens and as a result have multiple databases with personal information (PI) and personal health information (PHI).

In addition, eHealth who is a health trustee and service provider has numerous databases containing PHI. The 12 health regions also hold PHI but they are being merged into a single health authority. For the purposes of this paper, my office has named it the "provincial health authority". My office understands the government will determine the final name of the authority.

Because there are risks with data matching, my office opted to be cautious in its proposals and limit data matching to government institutions, eHealth Saskatchewan and the "provincial health authority". My office's proposals also prohibit data matching except as done under the provisions of the proposed legislation.

Section 29 of *The Health Information Protection Act (*HIPA) and section 29 of *The Provincial Archives and Public Records Management Act* deal with research done by researchers internal or external to an organization. The proposals here do not change the existing legislation on doing research. The proposals are strictly narrowed to deal with government institutions, eHealth Saskatchewan or the "provincial health authority". It is understood that researchers in these organizations may require data matching and if they do, the organization for which they are doing research would have to comply with the legislation when passed.

When public bodies wish to data match, it is important to have a clear statement of the purpose of the data matching project. Merely saying, we want to find out what we can find out isn't sufficient. Statements which clearly define what the public body wants to achieve are essential. What problem do they wish to solve? What crisis do they wish to prevent? What plan do they wish to test? What program do they wish to evaluate? Thus, the legislation should require government institutions, eHealth Saskatchewan or the "provincial health authority" to clearly state the purpose of the data matching program.

As indicated, the proposals adopt a cautious approach. That cautious approach involves requiring some oversight of data matching activities. The province needs to reap the benefits of data matching without any of the risks of major intrusions into citizen's privacy. The proposals contemplate submitting documentation to my office prior to embarking on a data matching project.

Finally, because databases hold people's PI and PHI - there is an entitlement to know what public bodies are doing with that information. There is a need for public bodies to be open and transparent. Thus, the legislation should require government institutions, eHealth Saskatchewan and the "provincial health authority" publishing their data matching plans by posting information on their website.

Principles to apply when preparing legislation

Any legislation in Saskatchewan should embrace the principles outlined below.

1. **Establishing Purpose**
   Government institutions, eHealth Saskatchewan and the provincial health authority should be able to clearly state the purpose of each data matching project prior to performing any data matching.

2. **Data Minimization**
   The least amount of identifiable information should be used for data matching projects.

3. **De-identification**
   When designing a data matching project, government institutions, eHealth Saskatchewan and the provincial health authority should consider if the purpose of a data matching project can be achieved using de-identified information. If so, then only de-identified information should be used.

4. **Accuracy**
   Government institutions, eHealth Saskatchewan and the provincial health authority should only use carefully selected data sets that contains accurate, complete, and up-to-date information should be used to avoid generating biased or discriminatory results.

5. **Openness**
   Government institutions, eHealth Saskatchewan and the provincial health authority should notify the individuals whose personal information is being used in a data matching project. They should also notify these individuals about any personal information that is being generated about them. Individuals should be able to gain access to their own personal information upon request.

6. **Establishing Safeguards**
   Government institutions, eHealth Saskatchewan and the provincial health authority should establish physical, administrative, and technology safeguards to prevent unauthorized access to personal information that is collected, used, disclosed, or generated in a data matching project.

Recommendations for Legislation

As a result, I recommend the government of Saskatchewan propose and the Legislative Assembly consider a stand-alone Act dealing with data matching which would have the following elements:

- A definition of data matching.
- Prohibition of data matching unless in accordance with the Act.
- Limiting data matching to government institutions, eHealth Saskatchewan and the provincial health authority.
- Requirements before starting a data matching project, including: 1) privacy impact assessment, 2) the definition of purpose and scope, 3) documenting in an agreement and 4) notifying the Commissioner of each project.
- Require destruction of data generated.
- Require information about data matching projects to be posted on website.
- Allow citizens to find out whether they are part of the data matching project.
- Require a report after data matching project is complete.

Schedule A
British Columbia

The Freedom of Information and Protection of Privacy Act (BC-FIPPA)

Data-linking initiatives
36.1 (1) A public body participating in a new or significantly revised data-linking initiative must comply with the regulations, if any, prescribed for the purposes of this subsection.

(2) If all the participants in a new or significantly revised data-linking initiative are a health care body, the ministry of the minister responsible for the administration of the Ministry of Health Act or a health-related organization as prescribed, then subsection (1) does not apply to the participants.

(3) For the purposes of subsections (1) and (2), a public body is participating in

(a) a new data-linking initiative if the data-linking initiative is implemented after the date this section comes into force, or

(b) a significantly revised data-linking initiative if the data-linking initiative is an existing data-linking initiative and a public body participating in that data-linking initiative expands it by doing one or more of the following:

(i) adding a public body or an agency that is not already a participant in the data-linking initiative;

(ii) adding a database that is not already a part of the data-linking initiative;

(iii) undertaking a purpose that is not already a purpose of the data-linking initiative;

(iv) using a type of technology that is not already a part of the data-linking initiative.

(4) Despite subsection (3) (a), a public body is not participating in a new data-linking initiative if, before the date this section comes into force, the public body has completed a written project plan respecting the data-linking initiative that states

(a) the objectives of the project,

(b) the costs and benefits of the project, and

(c) the risks associated with those costs and benefits.

…

General Information respecting use of personal information
69(5) The head of a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(5.1) The head of a ministry, with respect to a proposed enactment, system, project, program or activity, must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the minister responsible for this Act for the minister's review and comment.

(5.2) If the minister responsible for this Act receives a privacy impact assessment under subsection (5.1) respecting a common or integrated program or activity or a data-linking initiative, the minister must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the commissioner for the commissioner's review and comment.

(5.3) The head of a public body that is not a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(5.4) The head of a public body that is not a ministry, with respect to a proposed system, project, program or activity, must submit, during the development of the proposed system, project, program or activity, the privacy impact assessment, if it addresses a common or integrated program or activity or a data-linking initiative, to the commissioner for the commissioner's review and comment.

(5.5) The head of a public body must notify the commissioner of a data-linking initiative or of a common or integrated program or activity at an early stage of developing the initiative, program or activity.

(5.6) If all the participants in a data-linking initiative are either a health care body, the ministry of the minister responsible for the administration of the Ministry of Health Act or a health-related organization as prescribed, then

(a) subsections (5.3), (5.4) and (5.5) do not apply with respect to a participant that is a health care body or a health-related organization as prescribed, and

(b) subsections (5), (5.1) and (5.5) do not apply with respect to a participant that is the ministry of the minister responsible for the administration of the Ministry of Health Act.

(5.7) The head of a ministry must prepare an information-sharing agreement in accordance with the directions of the minister responsible for this Act.

(6) The head of a public body that is not a ministry must make available for inspection and copying by the public a directory that lists the public body's personal information banks and includes the following information with respect to each personal information bank:

(a) its title and location;

(b) a description of the kind of personal information and the categories of individuals whose personal information is included;

(c) the authority for collecting the personal information;

(d) the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed;

(e) the categories of persons who use the personal information or to whom it is disclosed;

(f) information required under subsection (7).

British Columbia's *Freedom of Information and Protection of Privacy Act* can be found at this link: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

Schedule B
Alberta

The Health Information Act (AB-HIA)

Prohibition
68 A custodian or health information repository must not

(a) collect the health information to be used in data matching, or

(b) use or disclose the health information to be used in data matching or created through data matching

in contravention of this Act.

Data matching by custodian or health information repository
69 A custodian or health information repository may perform data matching using information that is in its custody or under its control.

Data matching by custodians or health information repository
70(1) A custodian or health information repository may perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of another custodian or health information repository.

(2) Before performing data matching under this section, the custodian or health information repository in whose custody and control the information that is created through data matching will be stored must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment.

(3) A privacy impact assessment referred to in subsection (2) must

(a) describe how the information to be used in the data matching is to be collected, and

(b) set out how the information that is created through data matching is to be used or disclosed.

Data matching by custodian or health information repository and non-custodian
71(1) A custodian or health information repository may perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of a person that is not a custodian or health information repository.

(2) Before performing data matching under this section, the custodian or health information repository must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment.

(3) A privacy impact assessment referred to in subsection (2) must meet the requirements of section 70(3).

Data matching for research
72 If data matching is performed for the purpose of conducting research, sections 48 to 56 must be complied with before the data matching is performed.

Alberta's *Health Information Act* can be found at this link http://www.qp.alberta.ca/documents/Acts/H05.pdf

Schedule C
New South Wales

The *Data Sharing (Government Sector) Act 2015* (NSW_DSGSA)

The Legislature of New South Wales enacts:

Part 1 Preliminary

1 Name of Act
This Act is the *Data Sharing (Government Sector) Act 2015*.

2 Commencement
This Act commences on the date of assent to this Act.

3 Objects of Act
The objects of this Act are:

(a) to promote, in a manner that recognises the protection of privacy as an integral component, the management and use of government sector data as a public resource that supports good Government policy making, program management and service planning and delivery, and

(b) to remove barriers that impede the sharing of government sector data with the DAC or between other government sector agencies, and

(c) to facilitate the expeditious sharing of government sector data with the DAC or between other government sector agencies, and

(d) to provide protections in connection with data sharing under this Act by:

(i) specifying the purposes for, and the circumstances in, which data sharing is permitted or required, and

(ii) ensuring that data sharing involving health information or personal information continues to be in compliance with the requirements of the privacy legislation concerning the collection, use, disclosure, protection, keeping, retention or disposal of such information, and

(iii) requiring compliance with data sharing safeguards in connection with data sharing.

4 Definitions
(1) In this Act:

control in relation to data—see subsection (2).

DAC means that part of the Department known as the Data Analytics Centre or such other government sector agency (or part of a government sector agency) as may be prescribed by the regulations.

data means any facts, statistics, instructions, concepts or other information in a form that is capable of being communicated, analysed or processed (whether by an individual or by a computer or other automated means).

data analytics work means the examination and analysis of data for the purpose of drawing conclusions about that data (including, for example, conclusions about the efficacy of Government policies, program management or service planning and delivery by government sector agencies).

data provider means the government sector agency that controls government sector data that is provided under this Act to a data recipient.

data recipient means the government sector agency to which government sector data is provided under this Act.

data sharing safeguards—see Part 3.

Department means the Department of Finance, Services and Innovation.

function includes a power, authority or duty, and ***exercise*** a function includes perform a duty

government sector agency means each of the following:

(a) the DAC,

(b) a government sector agency within the meaning of the *Government Sector Employment Act 2013*,

(c) a statutory body representing the Crown,

(d) a council or county council within the meaning of the *Local Government Act 1993*,

(e) a State owned corporation,

(f) a body (whether incorporated or unincorporated) established or continued for a public purpose by or under the provisions of an Act or statutory instrument,

(g) a wholly-owned subsidiary of the Crown in right of the State or an agency, council, corporation or other body referred to in paragraph (a), (b), (c), (d), (e) or (f),

(h) a person or body exercising public official functions declared by the regulations to be a government sector agency for the purposes of this Act.

government sector data means any data that a government sector agency controls, but does not include data of a kind excluded by the regulations.

head of a government sector agency means:

(a) in the case of a government sector agency within the meaning of the *Government Sector Employment Act 2013*—the head of the agency within the meaning of that Act, and

(b) in the case of any other government sector agency:

(i) the chief executive officer or other principal officer of the agency, or

(ii) any other person who is declared by the regulations to be the head of the agency for the purposes of this definition.

health information has the same meaning as in the *Health Records and Information Privacy Act 2002*.

personal information has the same meaning as in the *Privacy and Personal Information Protection Act 1998*.

Note. Section 4A of the *Privacy and Personal Information Protection Act 1998* excludes health information from the definition of ***personal information*** in section 4 of that Act.

privacy legislation means:

(a) the *Privacy and Personal Information Protection Act 1998* or the *Health Records and Information Privacy Act 2002*, and

(b) any regulation or code of practice made, and any public interest directions or guidelines issued, under either of those Acts.

share, in relation to government sector data, means to provide (or be provided with) the data.

(2) For the purposes of this Act, a person or body is taken to have ***control*** of data if:

(a) the person or body has possession or custody of the data, or

(b) the person or body has the data in the possession or custody of some other person or body.

A person or body is, for example, taken to have control of data held by the person or body in storage with a commercial storage provider (including a storage provider who provides cloud storage facilities).

(3) Notes included in this Act do not form part of this Act.

5 Relationship of Act with other laws

(1) Subject to subsection (2), a disclosure of government sector data by a government sector agency to the DAC or to another government sector agency is lawful for the purposes of any other Act or law that would otherwise operate to prohibit that disclosure (whether or not the prohibition is subject to specified qualifications or exceptions) if:

(a) this Act provides that the agency is authorised to share the data with the DAC or other government sector agency, and

(b) the agency provides the data to the data recipient only for the purpose to which the authorisation to share relates.

(2) Nothing in this Act authorises, permits or requires the DAC or another government sector agency:

(a) to collect, use, disclose, protect, keep, retain or dispose of any government sector data that is health information or personal information otherwise than in compliance with the privacy legislation, or

(b) to disclose any government sector data that is:

(i) excluded information of an agency specified in Schedule 2 to the *Government Information (Public Access) Act 2009* (being any information that relates to any function specified in that Schedule in relation to the agency), or

(ii) information of a kind described in Schedule 1 to that Act, or

(c) to deal with any government sector data to which the *State Records Act 1998* applies after it is shared under this Act otherwise than in compliance with the *State Records Act 1998*.

(3) This Act is not intended to prevent or discourage the sharing of government sector data by government sector agencies as permitted or required by or under any Act or other law (apart from this Act).

Part 2 Facilitating government sector data sharing

6 Voluntary data sharing with DAC or between other government sector agencies

(1) A government sector agency (other than the DAC) is, subject to section 5 (2), authorised to share government sector data that it controls with the DAC or with another government sector agency for any of the following purposes:

(a) to enable data analytics work to be carried out on the data to identify issues and solutions regarding Government policy making, program management and service planning and delivery by the government sector agencies,

(b) to enable related government sector agencies (such as branches, offices and other agencies within or otherwise related to a Public Service agency) to develop better Government policy making, program management and service planning and delivery by the agencies,

(c) such other purposes as may be prescribed by the regulations.

(2) If government sector data is shared under this section, the data provider and the data recipient must comply with all data sharing safeguards that are applicable to them in connection with the sharing.

7 Minister may give directions for data sharing with DAC

(1) The Minister may direct a government sector agency in writing to provide specified government sector data that it controls to the DAC within 14 days or such longer period specified in the direction, but only if the Premier has advised the Minister that the data concerned is required to be shared for the purpose of advancing a Government policy.

(2) A copy of a direction given under this section must be provided to the head of the government sector agency to which the direction is given.

(3) If a direction is given under this section:

(a) the specified data provider is, subject to section 5 (2), authorised and required to provide the specified government sector data in compliance with the direction, and

(b) the specified data provider and the DAC must comply with all data sharing safeguards that are applicable to them in connection with the sharing of the data.

(4) The Premier may certify, in writing, that the Premier has advised the Minister that a specified provision of government sector data by a government sector agency is required for the purpose of advancing a Government policy. The certificate is conclusive evidence of the matter stated in the certificate.

(5) The head of a government sector agency to which a direction is given under this section must ensure that the direction is complied with in accordance with subsection (3).

(6) A direction cannot be given under this section to a government sector agency that is a university.

8 Minister may obtain information for DAC concerning government sector data sets

(1) The Minister may direct a government sector agency in writing to provide the DAC with such information concerning the government sector data that it controls as the Minister may require so as to enable the DAC to determine the number and kinds of sets of data that the agency controls and the kind of information collected in those data sets.

(2) A copy of a direction given under this section must be provided to the head of the government sector agency to which the direction is given.

(3) The government sector agency is (subject to section 5 (2)) authorised and required to comply with a direction given to it under this section.

(4) This section does not require a government sector agency to provide government sector data to the DAC.

(5) Nothing in this section affects or limits the functions of the Privacy Commissioner under the privacy legislation.

9 Sharing of results of data analytics work carried out by the DAC
The DAC is, subject to section 5 (2), authorised to share with government sector agencies the results of data analytics work that it has carried out on data provided to it by a government sector agency under this Act, but is not authorised to share that data with any other agency, person or body.

10 Directions to State owned corporations
(1) A direction may be given under this Part to a State owned corporation only if:

(a) the direction is given with the approval of the Premier, and

(b) where the portfolio Minister of the State owned corporation is neither the Premier nor the Minister administering this Act—the Minister administering this Act has consulted the portfolio Minister about the direction before it is given.

(2) If the direction to provide the government sector data is given in circumstances where the board of the State owned corporation considers that it is not in the commercial interests of the State owned corporation to provide the data, a State owned corporation is entitled to be reimbursed for the activity of providing the data in accordance with the provisions of section 20N (3)–(5) of the *State Owned Corporations Act 1989*.

(3) In this section:

portfolio Minister, in relation to a State owned corporation, has the same meaning as in the *State Owned Corporations Act 1989*.

Part 3 Data sharing safeguards

11 The data sharing safeguards
This Part sets out the ***data sharing safeguards*** for the purposes of this Act that are applicable to the sharing of government sector data under this Act with the DAC or between other government sector agencies.

12 Privacy safeguards
(1) Without limiting section 5 (2), a data provider and data recipient must ensure that health information or personal information contained in government sector data that is shared is not collected, used, disclosed, protected, kept, retained or disposed of otherwise than in compliance with the privacy legislation.

(2) If a data recipient that is provided with government sector data that contains health information or personal information becomes aware that the privacy legislation has been (or is likely to have been) contravened in relation to that information while in the recipient's control, the data recipient must, as soon as is practicable after becoming aware of it, inform the data provider and the Privacy Commissioner of the contravention or likely contravention.

13 Confidentiality and commercial-in-confidence
(1) A data recipient that is provided with government sector data that contains confidential or commercially sensitive information must ensure that the information is dealt with in a way that complies with any contractual or equitable obligations of the data provider concerning how it is to be dealt with.

(2) In this section:

confidential or commercially sensitive information means:

(a) information a person or body controls that the person or body is required to keep confidential because of a contractual or equitable obligation, or

(b) without limiting paragraph (a), information about commercial-in-confidence provisions of a contract (within the meaning of the *Government Information (Public Access) Act 2009*), or

(c) any other information the disclosure of which would prejudice any person's legitimate business, commercial, professional or financial interests.

14 Data custody and control safeguards
(1) A data provider and data recipient must ensure that the government sector data that is shared is maintained and managed in compliance with any legal requirements concerning its custody and control (including, for example, requirements under the *Government Information (Public Access) Act 2009* or *State Records Act 1998*) that are applicable to them.

(2) If a data recipient that arranges for a person or body (other than another government sector agency) to conduct data analytics work using government sector data with which it has been provided, the head of the data recipient is to ensure that appropriate contractual arrangements are in place before the data is provided to ensure that the person or body deals with the data in compliance with any requirements of the privacy legislation, the *State Records Act 1998* and any Government data security policies that are applicable to the data recipient.

Note. See, also, the offences in Part 6 of the *Crimes Act 1900* in connection with unauthorised access to, or the modification or impairment of, data held in computers.

15 Other data sharing safeguards
(1) A data provider and data recipient must comply with such other requirements as may be prescribed by the regulations for the provider or recipient in connection with the sharing of government sector data.

(2) Without limiting subsection (1), a requirement prescribed by the regulations for the purposes of that subsection may require a data provider or data recipient to comply with any of the following in connection with the sharing of government sector data:

(a) specified instruments, or specified provisions of instruments, forming part of the privacy legislation (for example, codes of practice, guidelines or directions),

(b) any other codes of practice, guidelines, directions or publications specified (or issued, made or published as provided) by the regulations.

New South Wales' *Data Sharing (Government Sector) Act 2015* can be found at this link:
http://www.legislation.nsw.gov.au/#/view/act/2015/60/full

Schedule D
New Zealand

The *Privacy Act 1993* (NZ-PA)

Part 10
Information matching

Interpretation

97 Interpretation
In this Part, unless the context otherwise requires,—

adverse action means any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual; and, without limiting the generality of the foregoing, includes any decision—

(a) to cancel or suspend any monetary payment:

(b) to refuse an application for a monetary payment:

(c) to alter the rate or amount of a monetary payment:

(d) to recover an overpayment of a monetary payment:

(e) to make an assessment of the amount of any tax, levy, or other charge, or of any contribution, that is payable by any individual, or to alter any such assessment:

(f) to investigate the possible commission of an offence:

(g) to make a deportation order in relation to the individual, to serve the individual with a deportation liability notice, or to deport the individual from New Zealand

authorised information matching information in relation to any specified agency, means information that consists of or includes information disclosed pursuant to an information matching provision

authorised information matching programme means the comparison (whether manually or by means of any electronic or other device) of authorised information matching information with other personal information for the purpose of producing or verifying information about an identifiable individual

discrepancy, in relation to an authorised information matching programme, means a result of that programme that warrants the taking of further action by any agency for the purpose of giving effect to the objective of the programme

information matching programme means the comparison (whether manually or by means of any electronic or other device) of any document that contains personal information about 10 or more individuals with 1 or more other documents that contain personal information about 10 or more individuals, for the purpose of producing or verifying information that may be used for the purpose of taking adverse action against an identifiable individual

information matching provision means any provision specified in the second column of Schedule 3 as an information matching provision of an enactment specified in the first column of that schedule

information matching rules means the rules for the time being set out in Schedule 4

monetary payment includes—

(a) a benefit within the meaning of section 3(1) of the Social Security Act 1964:

(b) a lump sum payable under section 61DB or section 61DC or section 61DD of that Act:

(c) any special assistance granted out of a Crown Bank Account from money appropriated by Parliament under section 124(1)(d) or (da) of that Act:

(d) any monetary entitlement payable under Part 4, Part 10, or Part 11 of the *Accident Compensation Act 2001*

specified agency means any of the following agencies:

(a) the Accident Compensation Corporation:

(aa) the Regulator, as defined by Part 10 of the Accident Compensation Act 2001:

(b) the Electoral Commission established by section 4B of the Electoral Act 1993:

(ba) the company within the meaning of section 2(1) of the Housing Restructuring and Tenancy Matters Act 1992:

(bb) the Board of the Government Superannuation Fund Authority:

(bc) the Board of Trustees of the National Provident Fund:

(bd) the Ministry of Health:

(c) the Ministry of Justice:

(d) the Department of Corrections:

(e) the Ministry of Business, Innovation, and Employment:

(f) the department for the time being responsible for the administration of the Social Security Act 1964:

(fa) the Housing New Zealand Corporation established (as the Housing Corporation of New Zealand) by section 3(1) of the Housing Corporation Act 1974:

(g) the Inland Revenue Department:

(ga) the Ministry of Transport:

(gb) the New Zealand Transport Agency:

(gc) the Department of Internal Affairs:

(gd) the Registrar-General appointed under section 79(1) of the Births, Deaths, Marriages, and Relationships Registration Act 1995:

(h) the New Zealand Customs Service:

(ha) the Registrar of Motor Vehicle Traders:

(i) the Regulator, as defined in the Accident Insurance Act 1998:

(ia) WorkSafe New Zealand:

(j) any tertiary institution, secondary school, or private training establishment (as those terms are defined in the Education Act 1989) to which section 226A or section 238B of that Act applies, as from time to time notified to the Commissioner by the department for the time being responsible for the administration of the Social Security Act 1964:

(k) the Ministry of Education:

(l) the Education Council of Aotearoa New Zealand established under Part 32 of the Education Act 1989:

(m) the agency or agencies appointed under section 100 of the Housing Restructuring and Tenancy Matters Act 1992.

Information matching guidelines

98 Information matching guidelines

The following matters are the matters referred to in section 13(1)(f) to which the Commissioner shall have particular regard, in examining any proposed legislation that makes provision for the collection of personal information by any public sector agency, or the disclosure of personal information by one public sector agency to any other public sector agency, in any case where the Commissioner considers that the information might be used for the purposes of an information matching programme:

(a) whether or not the objective of the programme relates to a matter of significant public importance:

(b) whether or not the use of the programme to achieve that objective will result in monetary savings that are both significant and quantifiable, or in other comparable benefits to society:

(c) whether or not the use of an alternative means of achieving that objective would give either of the results referred to in paragraph (b):

(d) whether or not the public interest in allowing the programme to proceed outweighs the public interest in adhering to the information privacy principles that the programme would otherwise contravene:

(e) whether or not the programme involves information matching on a scale that is excessive, having regard to—

(i) the number of agencies that will be involved in the programme; and

(ii) the amount of detail about an individual that will be matched under the programme:

(f) whether or not the programme will comply with the information matching rules.

Authorised information matching programmes

99 Information matching agreements

(1) No personal information held by any specified agency shall be disclosed, pursuant to an information matching provision, to any other specified agency for the purposes of an authorised information matching programme except pursuant to a written agreement between those agencies.

(2) Every such agreement shall incorporate provisions that reflect the information matching rules, or provisions that are no less onerous than those rules, and the agencies that are parties to the agreement shall comply with those provisions.

(3) Any such agreement may provide that the agencies involved in the information matching programme may charge each other fees for the services provided for the purposes of the programme.

(4) The parties to an agreement entered into pursuant to this section shall ensure that a copy of the agreement, and of any amendments subsequently made to such an agreement, are forwarded to the Commissioner forthwith.

Compare: 1991 No 126 s 14

100 Use of results of information matching programme

(1) Subject to any other enactment or rule of law that limits or restricts the information that may be taken into account in taking adverse action against an individual, any specified agency that is involved in an authorised information matching programme may take adverse action against an individual on the basis of any discrepancy produced by that programme.

(2) Nothing in subsection (1) shall be taken to limit or restrict the use that may lawfully be made, by any specified agency, of any information produced by an authorised information matching programme.

Compare: 1991 No 126 s 15; Data-matching Program (Assistance and Tax) Act 1990 s 10(1) (Aust)

101 Further provisions relating to results of information matching programme

(1) Notwithstanding anything in section 100, where—

(a) a specified agency derives or receives information produced by an authorised information matching programme; and

(b) as a result of deriving or receiving that information, the agency becomes aware of a discrepancy,—

that agency shall destroy that information not later than the expiration of the period of 60 working days after the agency becomes aware of that discrepancy unless, before the expiration of that period, the agency has considered that information and made a decision to take adverse action against any individual on the basis of that discrepancy.

(2) Any adverse action commenced by a specified agency in accordance with subsection (1) shall be commenced not later than 12 months from the date on which the information was derived or received by the agency.

(3) Where a specified agency decides not to take adverse action against any individual on the basis of information produced by an authorised information matching programme, the agency shall as soon as practicable destroy the information.

(4) When information produced by an authorised information matching programme is no longer needed by a specified agency for the purposes of taking any adverse action against any individual, the agency shall as soon as practicable destroy the information.

(5) Nothing in this section applies in relation to the Inland Revenue Department.

102 Extension of time limit

Where a specified agency derives or receives information produced by an authorised information matching programme, the Commissioner may, either generally or in respect of any case or class of cases, extend the time limit set out in section 101 in respect of that information if the Commissioner is satisfied that,—

(a) because of the large quantity of information so derived or received by the agency; or

(b) because of the complexity of the issues involved; or

(c) for any other reason,—

the agency cannot reasonably be required to meet the time limit.

103 Notice of adverse action proposed

(1) Subject to subsections (1A) to (2A) and to section 180C(1) of the Corrections Act 2004, a specified agency shall not take adverse action against any individual on the basis (whether wholly or in part) of a discrepancy produced by an authorised information matching programme—

(a) unless that agency has given that individual written notice—

(i) specifying particulars of the discrepancy and of the adverse action that it proposes to take; and

(ii) stating that the individual has 5 working days from the receipt of the notice in which to show cause why the action should not be taken; and

(b) until the expiration of those 5 working days.

(1A) Nothing in subsection (1) shall prevent the department for the time being responsible for the administration of the Social Security Act 1964 from immediately suspending sole parent support, the supported living payment, an emergency benefit, jobseeker support, a young parent payment, or a youth payment, paid to an individual where the discrepancy arises in respect of departure information supplied to that department pursuant to section 280 of the Customs and Excise Act 1996, and where, before or immediately after the decision to suspend, the department gives the individual written notice—

(a) specifying particulars of the discrepancy and the suspension of benefit, and any other adverse action the department proposes to take; and

(b) stating that the individual has 5 working days from the receipt of the notice to show cause why the benefit ought not to have been suspended or why the adverse action should not be taken, or both—

and the adverse action shall not be taken until the expiration of those 5 working days.

(1B) Nothing in subsection (1) prevents the Commissioner of Inland Revenue from immediately suspending payment to an individual of all or part of an interim instalment of a credit of tax under subparts MA to MF and MZ of the Income Tax Act 2007 when a discrepancy is identified in information supplied to the Commissioner under section 85G of the Tax Administration Act 1994 if, before or immediately after the decision to suspend, the Commissioner gives a written notice to the individual that—

(a) provides details of the discrepancy and the suspension of payment of the credit of tax and any other adverse action which the Commissioner proposes to take; and

(b) states that the individual has 5 working days from the receipt of the notice to show cause why payment of the credit of tax ought not to have been suspended or why the adverse action should not be taken, or both—

and the other adverse action must not be taken until expiration of those 5 working days.

(1C) Nothing in subsection (1) prevents the Commissioner of Inland Revenue from immediately taking action to recover amounts relating to—

(a) unpaid amounts owed to the Commissioner by an individual who is in serious default identified in information supplied to the Commissioner under section 280H of the Customs and Excise Act 1996; or

(b) financial support under the Child Support Act 1991 owed to the Commissioner by an individual who is identified in information supplied to the Commissioner under section 280K or 280L of the Customs and Excise Act 1996.

(2) Nothing in subsection (1) or subsection (1A) or subsection (1B) prevents an agency from taking adverse action against an individual if compliance with the requirements of that subsection would prejudice any investigation into the commission of an offence or the possible commission of an offence.

(2A) Nothing in subsection (1) prevents any constable or any bailiff from immediately executing a warrant to arrest an individual in respect of the non-payment of the whole or any part of a fine if the discrepancy arises in respect of arrival and departure information supplied under section 280D of the Customs and Excise Act 1996 and if, before executing the warrant, the individual concerned is—

(a) informed of the intention to execute the warrant; and

(b) given an opportunity to confirm—

(i) whether or not he or she is the individual named in the warrant; and

(ii) that neither of the following circumstances applies:

(A) the fine has been paid:

(B) an arrangement to pay the fine over time has been entered into.

(3) Every notice required to be given to any individual under subsection (1) or subsection (1A) or subsection (1B) may be given by delivering it to that individual, and may be delivered—

(a) personally; or

(b) by leaving it at that individual's usual or last known place of residence or business or at the address specified by that individual in any application or other document received from that individual; or

(c) by posting it in a letter addressed to that individual at that place of residence or business or at that address.

(4) If any such notice is sent to any individual by post, then in the absence of proof to the contrary, the notice shall be deemed to have been delivered to that individual on the fourth day after the day on which it was posted, and in proving the delivery it shall be sufficient to prove that the letter was properly addressed and posted.

(5) In this section,—

amount of reparation has the same meaning as in section 79 of the Summary Proceedings Act 1957

bailiff means a bailiff of the District Court or of the High Court

fine means—

(a) a fine within the meaning of section 79 of the Summary Proceedings Act1957:

(b) a fine to which section 19 of the Crimes Act 1961 applies:

(c) a fine to which section 43 or 45 of the Misuse of Drugs Amendment Act

1978 applies:

(d) ***[Repealed]***

(e) any amount payable under section 138A(1) of the Sentencing Act 2002.

104 Reporting requirements

(1) Every specified agency that is involved in an authorised information matching programme shall make such reports to the Commissioner in respect of that programme as the Commissioner may from time to time require.

(2) Without limiting the generality of subsection (1), the matters on which the Commissioner may require any agency to submit a report include the following:

(a) the actual costs and benefits of an authorised information matching programme:

(b) any difficulties experienced in the operation of an authorised information matching programme, and how those difficulties are being, or have been, overcome:

(c) whether or not internal audits or other forms of assessment are undertaken by an agency in relation to an authorised information matching programme, and, if so, the results of those audits or assessments:

(d) where an agency dispenses with the giving of notice under section 103, the reasons why such a dispensation is made, and the grounds in support of those reasons:

(e) the details of the operation of an authorised information matching programme, including—

(i) the number of matches undertaken:

(ii) the proportion of matches that revealed discrepancies in information involved in the matching:

(iii) the number of discrepancies so revealed:

(iv) the proportion of cases in which action was taken as a result of such discrepancies:

(v) the number of cases in which such action was taken:

(vi) the number of cases in which such action was taken even though the accuracy of the discrepancy was challenged:

(vii) the proportion of cases in which such action did not proceed after the individual concerned was notified of the discrepancy:

(viii) the number of cases in which action taken as a result of a discrepancy was successful:

(f) such other matters as the Commissioner considers relevant.

105 Information matching programmes to be reported on in annual report

(1) The Commissioner shall include in every annual report of the Commissioner under section 150 of the Crown Entities Act 2004, in relation to each authorised information matching programme that is carried out (in whole or in part) during the year to which the report relates,—

(a) an outline of the programme; and

(b) an assessment of the extent of the programme's compliance, during that year, with—

(i) sections 99 to 103; and

(ii) the information matching rules; and

(c) the details of each extension granted under section 102, the reasons why the extension was granted, and the grounds in support of those reasons; and

(d) the details of each approval given, during that year, under clause 3 of Schedule 4, the reasons why the approval was given, and the grounds in support of those reasons.

(2) Nothing in subsection (1) requires the Commissioner to include in any annual report, in respect of any authorised information matching programme, any information the disclosure of which would be likely to frustrate the objective of the programme.

(3) For the purposes of carrying out any assessment required by subsection (1)(b), Part 9 shall apply, with such modifications as are necessary, as if the assessment were an investigation under Part 8.

106 Review of statutory authorities for information matching

(1) As soon as practicable after 1 January 1994, and then at intervals of not more than 5 years, the Commissioner shall—

(a) review the operation of every information matching provision since—

(i) 19 December 1991 (in the case of the first review carried out under this paragraph); or

(ii) the date of the last review carried out under this paragraph (in the case of every subsequent review); and

(b) consider whether or not, in the Commissioner's opinion,—

(i) the authority conferred by the information matching provision should be continued; and

(ii) any amendments to the provision are necessary or desirable; and

(c) report the Commissioner's findings to the responsible Minister.

(2) As soon as practicable after receiving a report from the Commissioner under subsection (1)(c), the responsible Minister shall lay a copy of that report before the House of Representatives.

107 Amendment of information matching rules

(1) For the purposes of this Part, the Governor-General may from time to time, by Order in Council, make such amendments to Schedule 4 as the Governor-General thinks fit.

(2) The power conferred by subsection (1) includes the power to repeal Schedule 4 and substitute a new schedule.

(3) No order that amends Schedule 4 shall be made otherwise than in accordance with the recommendations of the Commissioner.

Avoidance of controls on information matching

108 Avoidance of controls on information matching through use of exceptions to information privacy principles

Where the collection or disclosure of information is authorised by an information matching provision, nothing in subclause (2)(d)(i) of principle 2 or paragraph (e)(i) of principle 11 authorises or permits the collection or disclosure of that information for the purposes of—

(a) any authorised information matching programme; or

(b) any information matching programme the objective of which is similar in nature to any authorised information matching programme.

109 Avoidance of controls on information matching through use of official information statutes
Notwithstanding anything in the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, no public sector agency shall disclose pursuant to either of those enactments, to any other public sector agency, any personal information if the sole or principal purpose for which that information is sought is for use in an information matching programme.

…

Schedule 4
Information matching rules

1 Notice to individuals affected
(1) Agencies involved in an authorised information matching programme shall take all reasonable steps (which may consist of or include public notification) to ensure that the individuals who will be affected by the programme are notified of the programme.

(2) Nothing in subclause (1) requires an agency to notify any individual about an authorised information matching programme if to do so would be likely to frustrate the objective of the programme.

2 Use of unique identifiers
Except as provided in any other enactment, unique identifiers shall not be used as part of any authorised information matching programme unless their use is essential to the success of the programme.

3 On-line transfers
(1) Except with the approval of the Commissioner, information transferred between agencies for the purposes of an authorised information matching programme shall not be transferred by means of on-line computer connections.

(2) Any approval given under subclause (1) may be given either unconditionally or subject to such conditions as the Commissioner thinks fit.

(3) Any approval given under subclause (1) may at any time be withdrawn by the Commissioner; and any condition subject to which any such approval is given may from time to time be revoked, varied, or added to by the Commissioner.

4 Technical standards
(1) The agency primarily responsible for the operation of an authorised information matching programme shall establish and maintain detailed technical standards to govern the operation of the programme.

(2) The technical standards established by an agency in accordance with subclause (1) shall deal with the following matters:

(a) the integrity of the information to be matched, with particular reference to—

(i) key terms and their definition; and

(ii) relevance, timeliness, and completeness:

(b) the matching techniques to be used in the programme, with particular reference to—

(i) the matching algorithm:

(ii) any use of unique identifiers:

(iii) the nature of the matters being sought to be identified by the matching process:

(iv) the relevant information definitions:

(v) the procedure for recognising matches:

(c) the controls being used to ensure the continued integrity of the programme, including the procedures that have been established to confirm the validity of matching results:

(d) the security features included within the programme to minimise and audit access to personal information, including the means by which the information is to be transferred between agencies.

(3) The technical standards established in accordance with subclause (1) shall be incorporated in a written document (in this clause called a Technical Standards Report), and copies of the Technical Standards Report shall be held by all agencies that are involved in the authorised information matching programme.

(4) Variations may be made to a Technical Standards Report by way of a Variation Report appended to the original report.

(5) The agency that prepares a Technical Standards Report shall forward a copy of that report, and of every Variation Report appended to that report, to the Commissioner.

(6) The Commissioner may from time to time direct that a Technical Standards Report be varied, and every such direction shall be complied with by the agency that prepared the report.

(7) Every agency involved in an authorised information matching programme shall comply with the requirements of the associated Technical Standards Report (including any variations made to the report).

5 Safeguards for individuals affected by results of programmes

(1) The agencies involved in an authorised information matching programme shall establish reasonable procedures for confirming the validity of discrepancies before any agency seeks to rely on them as a basis for action in respect of an individual.

(2) Subclause (1) shall not apply if the agencies concerned consider that there are reasonable grounds to believe that the results are not likely to be in error, and in forming such a view regard shall be had to the consistency in content and context of the information being matched.

(3) Where such confirmation procedures do not take the form of checking the results against the source information, but instead involve direct communication with the individual affected, the agency that seeks to rely on the discrepancy as a basis for action in respect of an individual shall notify the individual affected that no check has been made against the information which formed the basis for the information supplied for the programme.

(4) Every notification in accordance with subclause (3) shall include an explanation of the procedures that are involved in the examination of a discrepancy revealed by the programme.

6 Destruction of information

(1) Personal information that is disclosed, pursuant to an information matching provision, to an agency for use in an authorised information matching programme and that does not reveal a discrepancy shall be destroyed as soon as practicable by that agency.

(2) Where—

(a) Personal information is disclosed, pursuant to an information matching provision, to an agency for use in an authorised information matching programme; and

(b) that information reveals a discrepancy,—

that information shall be destroyed by that agency as soon as practicable after that information is no longer needed by that agency for the purposes of taking any adverse action against any individual.

(3) Nothing in this clause applies in relation to the Inland Revenue Department.

7 No new databank

(1) Subject to subclauses (2) and (3), the agencies involved in an authorised information matching programme shall not permit the information used in the programme to be linked or merged in such a way that a new separate permanent register or databank of information is created about all or any of the individuals whose information has been subject to the programme.

(2) Subclause (1) does not prevent an agency from maintaining a register of individuals in respect of whom further inquiries are warranted following a discrepancy revealed by the programme, but information relating to an individual may be maintained on such a register only for so long as is necessary to enable those inquiries to be carried out, and in no case longer than is necessary to enable any adverse action to be taken against an individual.

(3) Subclause (1) does not prevent an agency from maintaining a register for the purpose of excluding individuals from being selected for investigation, but such register shall contain the minimum amount of information necessary for that purpose.

8 Time limits

(1) Where an authorised information matching programme is to continue for any period longer than 1 year, or for an indefinite period, the agencies involved in the programme shall establish limits on the number of times that matching is carried out pursuant to the programme in each year of its operation.

(2) The limits established in accordance with subclause (1) shall be stated in writing in an annex to the Technical Standards Report prepared in respect of the programme pursuant to clause 4.

(3) The limits established in accordance with subclause (1) may be varied from time to time by the agencies involved in the programme.

New Zealand's *Privacy Act 1993* can be found at this link:
http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296645.html?search=ts_act%40bill%40regulation%40deemedreg_privacy+act_resel_25_a&p=1

Schedule E
European Union

European Union's *General Data Protection Regulation* (EU-GDPR)

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

   (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

   (b) the contact details of the data protection officer, where applicable;

   (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

   (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

   (e) the recipients or categories of recipients of the personal data, if any;

   (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

   (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

   (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

   (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

   (d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

…

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless

otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

The *EU's General Data Protection Regulations* can be found at this link:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf