



New Zealand
Security Intelligence
Service
Te Pā Whakamarumarū



Te Tari Taiwhenua
Internal Affairs

DIRECT ACCESS AGREEMENT

UNDER THE

INTELLIGENCE AND SECURITY ACT 2017

BETWEEN

**THE MINISTER RESPONSIBLE FOR THE NEW ZEALAND SECURITY
INTELLIGENCE SERVICE (NZSIS)**

AND

THE MINISTER OF INTERNAL AFFAIRS

RELATING TO

**DIRECT ACCESS BY NZSIS TO BIRTH, DEATH, MARRIAGE, CIVIL
UNION AND NAME-CHANGE INFORMATION HELD BY THE
REGISTRAR-GENERAL**

1. Parties

- 1.1. This direct access agreement (DAA) is between the Minister Responsible for the New Zealand Security Intelligence Service (NZSIS) and the Minister of Internal Affairs (together the Parties).
- 1.2. This DAA comes into force on the date of the last signature.

2. Background and purpose

- 2.1. The Intelligence and Security Act 2017 (the ISA) enables an intelligence and security agency to have Direct Access to certain specified information contained on certain public sector databases. One of these databases is the BDM Database held by the Registrar-General which contains information relating to Births, Deaths, Marriages, Civil unions and Name-changes (BDMI).
- 2.2. Birth, death, marriage, civil union and name change records are a public register. Generally any verifiable individual can request copies of information from the public register, whether relating to their own personal information or relating to another. The request must be in respect of a named person, be supported by evidence of identity of the requestor, be supported by an application and payment of a fee.
- 2.3. The purpose of this DAA is to enable Direct Access by NZSIS (as an intelligence and security agency) to the BDM Database to collect and use BDMI.

3. Definitions

- 3.1. Terms relevant to this DAA are defined as follows:
 - 3.1.1. **Authorised Officers** means any NZSIS officer who has been certified by NZSIS's Compliance Manager as a) having a need to access BDMI for one or more of the purposes in clause 6, in order to carry out one of NZSIS's statutory functions, duties or powers in clause 7 of this DAA and b) having completed all of the necessary training and certification requirements to access the database.
 - 3.1.2. **BDMI** means information relating to births, deaths, marriages, civil unions and name-changes. It excludes all other information stored on the BDM database. For the avoidance of doubt, BDMI does not include adoption information, witness protection name change information, sexual assignment or correction information to which s77(2),(3) or (4) of the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMR) applies, or Human Assisted Reproductive Technology Act 2004 donor or donor offspring information.
 - 3.1.3. **Direct Access**, in relation to the BDM Database, means to do either or both of the following (whether remotely or otherwise):
 - 3.1.3.1. Search the database (by way of the BDM database query facilities); or
 - 3.1.3.2. Copy any information stored on the database (including by previewing, cloning, or other forensic methods).

- 3.1.4. **BDM Database** means the series of statutory registers held by the Registrar-General in accordance with the BDMR, which contain BDMI, including:
- 3.1.4.1. all of its computer components, including software, underlying data repositories, and any system interface required to access the database information.
- 3.1.5. **Registrar-General**, means the Registrar-General appointed under section 79(1) of the BDMR.
- 3.2. All of the other terms in this DAA (including BDMI) have the meaning as described in the ISA unless otherwise noted.

4. Database to be accessed

- 4.1. The database to be accessed is the BDM database.

5. Particular information that may be accessed

- 5.1. The information that NZSIS can access is all BDMI in the BDM Database, excluding any BDMI that is subject to any specific caveats placed on that information by the Registrar-General.

6. Particular purpose or purposes for which the information may be accessed

- 6.1. NZSIS may have Direct Access to BDMI contained on the BDM Database in accordance with the NZSIS's statutory objectives (the ISA, s 9), and its functions and powers specified below in clause 7 for the following purposes:
- 6.1.1. Identifying persons of security or intelligence interest and their familial details by obtaining and corroborating their biographical or familial details and/or the details of family members (i.e. intelligence collection and analysis);
- 6.1.2. obtaining and corroborating the biographical or familial details of persons seeking a national security clearance, national security check or any other access, activity or appointment which requires NZSIS (or in which NZSIS is requested) to provide national security advice (i.e. protective security services, advice and assistance); and
- 6.1.3. searching BDMI contained on the BDM Database (in accordance with clause 3.1.3.1) to ensure NZSIS does not create or amend an assumed identity (or request the Department of Internal Affairs (DIA) to create or amend an assumed identity) which is an exact match with someone of the same name and birth date born in New Zealand (i.e. request for assistance to acquire, use and maintain an assumed identity; Ministerial Policy Statement – Acquiring, using and maintaining an assumed identity).
- 6.2. Additional operational context on the purposes for which NZSIS may have Direct Access to BDMI is outlined in a classified Privacy Impact Assessment (PIA). That PIA is

the document titled NZSIS Privacy Impact Assessment Report, approved contemporaneously with this DAA.

7. Particular function or power being, or to be, performed or exercised by NZSIS for which the information is required

- 7.1. NZSIS may have Direct Access to BDMI to perform the following statutory functions and powers:
- 7.1.1. Intelligence collection and analysis;
 - 7.1.1 Protective security services, advice and assistance;
 - 7.1.2 Acquiring, use or maintenance of an assumed identity; and
 - 7.1.3 Request for assistance to acquire, use and maintain an assumed identity.
- 7.2 Additional Information on how BDMI will be used to perform these statutory functions and powers is outlined in the PIA.

8. Mechanism by which information is accessed

- 8.1. NZSIS may have Direct Access to the BDM Database through dedicated BDM Database terminals accessible only to Authorised Officers. BDMI must be assessed at the time of access as relevant for NZSIS purposes before it can be extracted, copied, and transferred to the NZSIS classified network.
- 8.2. Detailed mechanisms by which NZSIS may have Direct Access to BDMI on the BDM Database are set out in the PIA.
- 8.3. Any material changes to these access mechanisms or the PIA must be notified to the Inspector-General of Intelligence and Security (IGIS) and the Privacy Commissioner (PC).

9. Positions of persons who may access the information

- 9.1. Direct Access to BDMI will be limited to persons who hold the position of Authorised Officer working directly on the functions and powers specified in clause 7 of this DAA, and for the purposes specified in clause 6 of this DAA, where access is required to carry out that function or power.
- 9.2. Prior to having Direct Access to BDMI, each NZSIS Authorised Officer must:
- 9.2.1. complete training on access to, use and disclosure of BDMI as required by the Registrar-General;
 - 9.2.2. complete training in legal and policy obligations relating to access to, use and disclosure of BDMI, and retention and record keeping obligations as required by the NZSIS Compliance Manager;
 - 9.2.3. undertake in writing that they:
 - 9.2.3.1. have completed the necessary training;

- 9.2.3.2. understand and will comply with all of their obligations;
- 9.2.3.3. will maintain the integrity of their individual access to BDMI; and
- 9.2.3.4. will advise the NZSIS Compliance Manager if their need for access to BDMI changes.

9.3. NZSIS and the Registrar-General will mutually agree in writing to a mechanism whereby the Authorised Officer requirements are set and managed, and unique access accounts are issued and deactivated.

9.4. NZSIS will maintain an up-to-date and accurate record of the identities of all Authorised Officers, details of all training undertaken, and copies of all certifications. NZSIS will ensure that authorised officers will undertake the necessary training and certification requirements to access the database at least every three years.

10. Records to be kept in relation to each occasion a database is accessed

10.1. Access to and use of BDMI itself will generate detailed audit log data within the BDM Database.

10.2. NZSIS must keep an up-to-date and accurate record of:

- 10.2.1. Every occasion each Authorised Officer accesses BDMI;
- 10.2.2. The reason the Authorised Officer accessed BDMI, and the necessity/justification for access; and
- 10.2.3. Any records obtained by NZSIS from the BDM Database.

10.3. NZSIS must maintain a record of the above information in a way that can be audited by the Registrar-General, the IGIS or the PC if requested.

10.4. NZSIS and the Registrar-General will undertake a joint audit of the operation of this DAA at least once per year, in accordance with a joint audit procedure. Should any previous audit identify issues of privacy concern the Registrar-General may require a further joint audit within a reasonable time. A copy of this audit report will be provided to the IGIS, and any issues of privacy concern will be provided to the PC.

10.5. The Registrar-General can also review access by Authorised Officers to BDMI at any time.

11. Safeguards to be applied for protecting particular information

11.1. Detailed safeguards by which BDMI will be protected by NZSIS are set out in the classified PIA. The security and privacy safeguards to be applied include:

11.1.1. General safeguards

- 11.1.1.1. All Authorised Officers are security vetted to the highest level (Top Secret Special).

- 11.1.1.2. All Authorised Officers receive training on their privacy and official information obligations.
- 11.1.1.3. All Authorised Officers are subject to the NZSIS and State Services Commission Codes of Conduct.
- 11.1.1.4. All Authorised Officers are required to sign an information access agreement, outlining acceptable and unacceptable uses of NZSIS systems and information, prior to any system access being granted.
- 11.1.1.5. All access to and use of NZSIS electronic systems, is logged and subject to system auditing to ensure that access to information is in accordance with legislative requirements, NZSIS policies, and the Authorised Officer's role.

11.1.2. Access to BDMI

- 11.1.2.1. Only NZSIS Authorised Officers may directly access BDMI.
- 11.1.2.2. Authorised officers may only access BDMI in accordance with one of the purposes set out in clause 6 of this DAA.
- 11.1.2.3. Authorised Officers may only transfer BDMI to the NZSIS database after determining that information to be relevant to one of NZSIS's functions and powers specified in clause 7 of this DAA.

11.1.3. Safeguards for access to BDMI obtained from the BDM Database and stored on NZSIS systems

- 11.1.3.1. Access to BDMI obtained from the BDM Database will be strictly controlled in accordance with international security standards for intelligence and security agencies.
- 11.1.3.2. BDMI obtained from the BDM Database will only be stored on and accessed via secure networks and systems, with all user accounts, access rights, and security authorisations proactively managed and controlled in line with international security standards for intelligence and security agencies and subject to audit as per 10.4.

12. NZSIS obligations relating to storage, retention, and disposal of information obtained from the database

- 12.1. All BDMI obtained from the BDM Database will be handled and stored in accordance with the appropriate security endorsements, caveats, and protective markings and in accordance with the New Zealand Government Protective Security Requirements.
- 12.2. Any specific BDMI that is copied into NZSIS systems and is used in support of NZSIS's statutory functions will be retained and managed as public records of NZSIS activities, in accordance with the Public Records Act 2005, with a default retention period of 25 years.

12.3. Disposal of BDMI obtained from the BDM Database will be conducted in accordance with the Public Records Act 2005 and any retention and disposal schedule which governs this action.

13. Circumstances in which the information may be disclosed to another agency (whether in New Zealand or overseas), and how that disclosure may be made

13.1. The ISA provides that NZSIS may share intelligence (and any analysis of that intelligence) with the Minister Responsible for the NZSIS, the Chief Executive of the Department of the Prime Minister and Cabinet and any person or class of persons, whether in New Zealand or overseas, authorised by the Minister Responsible for the NZSIS to receive that intelligence (or analysis). The ISA imposes an additional requirement in relation to the provision of intelligence to any overseas person or class of persons, being that the Minister Responsible for the NZSIS must be satisfied that, in providing the intelligence, NZSIS will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

13.2. The Minister Responsible for the NZSIS has given Ministerial Authorisation to NZSIS to share intelligence, however that Authorisation is classified. For the purposes of the DAA, it is sufficient to note that the Ministerial Authorisation authorises NZSIS to provide intelligence, and any analysis of that intelligence, to:

13.2.1. any New Zealand Government agency including Parliament, the State Sector, Crown Entities, State Owned Enterprises, local government, and other specified government agencies and associated entities;

13.2.2. a number of specified overseas public authorities (including agencies from Australia, Canada, the United Kingdom and the United States of America); and

13.2.3. other specified persons in specified circumstances.

13.3. In accordance with the ISA, NZSIS will only disclose BDMI where doing so:

13.3.1. will contribute to one of NZSIS's statutory objectives (e.g. contribute to the protection of national security);

13.3.2. falls within one of NZSIS's statutory functions, duties or powers;

13.3.3. is to a person or class of persons (whether in New Zealand or overseas) authorised by the Minister Responsible for NZSIS to receive intelligence and any analysis of that intelligence; and

13.3.4. would not lead to a human rights breach.

13.4. Disclosures of BDMI will be made in accordance with the New Zealand Government's Protective Security Requirements and international security standards for intelligence and security agencies, and may be made verbally, electronically or in person.

13.5. In addition to the above, when sharing intelligence with external parties NZSIS gives consideration to overarching principles as outlined in internal policy, including the need to consider whether the interaction aligns with NZSIS objectives and NZ

Government Priorities; the necessity and proportionality of sharing personal information; human rights obligations; and whether the sharing is otherwise restricted or prohibited in any way.

14. Apportionment of costs

- 14.1. All costs associated with collecting, processing and storing BDMI within the BDM Database remains the sole responsibility of the Registrar-General.
- 14.2. All costs associated with NZSIS's access to BDMI within the BDM Database, including any costs associated with building a user interface, will be the joint responsibility of NZSIS and the Registrar-General.
- 14.3. All costs associated with the collection of BDMI following its extraction from the BDM Database, as well as the subsequent processing, storage, access and disposal within NZSIS systems remains the sole responsibility of NZSIS.
- 14.4. All costs associated with dealing with a breach of this agreement will be met by the party responsible for the breach occurring.

15. Consultation with IGIS and PC

- 15.1. Before entering into this DAA, the Parties consulted with and invited comment from the IGIS and the PC. The Parties took into account and had regard to the comments by the IGIS and PC.

16. Publication of this agreement

- 16.1. This DAA will be published on the NZCS and DIA websites.
- 16.2. The PIA is classified so will not be published, and may be withheld in accordance with the Official Information Act 1982.

17. Relationship with other legislation

- 17.1. Nothing in this agreement affects NZSIS's ability to request information, or the Registrar-General's ability to disclose information under the ISA, BDMR or any other enactment, however access to BDMI via this DAA is to be preferred unless there is good reason to request the information via other means.
- 17.2. Nothing in this DAA affects an individual's right to make an information privacy request in accordance with the Privacy Act 1993.
- 17.3. Nothing in this DAA affects an individual's right to make a complaint to the IGIS or to the PC.
- 17.4. Both Parties agree to keep each other informed of any complaints arising from the use of the BDM Database.

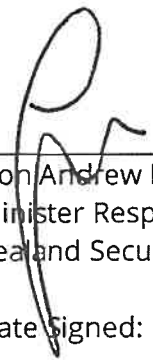
18. Dispute resolution

- 18.1 In the event of dispute the Parties will consult, through their nominated organisational representatives, with a view to resolving any issues as soon as practicable. If the dispute cannot be resolved, it will be escalated to the Chief Legal Advisers of each organisation or the Chief Executives for resolution.
- 18.2 Pending resolution of any dispute the Registrar-General may, with a reasonable period of notice to NZSIS, suspend any Authorised Officer's access to the BDM Database.

19. Review of this agreement

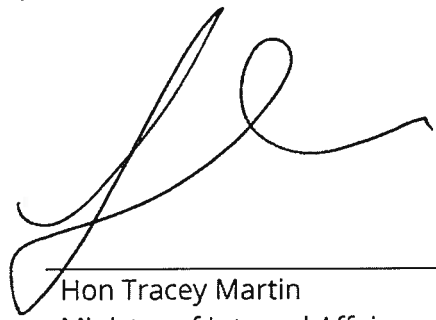
- 19.1. This DAA must be reviewed by the Minister Responsible for the NZSIS and the Minister of Internal Affairs within three years. This DAA can also be reviewed or amended (in accordance with the ISA) without the requirement to wait for three years.

Signed



Hon Andrew Little
Minister Responsible for the New
Zealand Security Intelligence Service

Date Signed: 3/10/18



Hon Tracey Martin
Minister of Internal Affairs

Date Signed: 3/12/18