Data Controller/Data Processor Memorandum of Understanding (MoU)

Service Requirements and Obligations

Between

Local Authority Name

and

National Records of Scotland
Contents

1. The Agreement ........................................................................................................................................... 4
   1.1. Statement of Intent .......................................................................................................................... 4
   1.2. Parties to the Agreement .................................................................................................................. 4
   1.3. Terms of Agreement ......................................................................................................................... 4
   1.4. Obligations ......................................................................................................................................... 4
   1.5. Document Sign-Off and Security ....................................................................................................... 4

2. The Service .................................................................................................................................................. 5
   2.1. Services in Scope and Description .................................................................................................... 5

3. Service Governance & Compliance ......................................................................................................... 5
   3.1. Governance Activities ...................................................................................................................... 5
   3.2. Compliance ......................................................................................................................................... 6
   3.3. Requirements ..................................................................................................................................... 6
   3.4. Data .................................................................................................................................................... 7
   3.5. Privacy and Confidentiality ............................................................................................................... 7
   3.6. Personal Data ..................................................................................................................................... 7
   3.7. Loss of Data ....................................................................................................................................... 8
   3.8. Ownership of Data ............................................................................................................................ 9
   3.9. Intellectual Property Rights .............................................................................................................. 9
   3.10. Records Retention ......................................................................................................................... 9
   3.12. Audit Rights ..................................................................................................................................... 10
   3.13. Quality Assurance ........................................................................................................................ 10
   3.14. Constraints ..................................................................................................................................... 10

4. Termination and Exit .................................................................................................................................. 10
   4.1. Termination Rights .......................................................................................................................... 10
   4.2. Termination Process and Responsibilities ........................................................................................ 10

5. Charging and Payments ............................................................................................................................. 11
6. Signatories
1. The Agreement

1.1. Statement of Intent

1.1.1. This document ("the Agreement") is a memorandum of understanding between the National Records of Scotland ("the Provider") and the Local Authority Name ("the Customer") in relation to the provision of data processing (including indexing) services by the Provider to the Customer and the legal requirements that the Provider must meet.

1.2. Parties to the Agreement

1.2.1. The Registrar General of Births, Deaths and Marriages for Scotland (the Provider) having its headquarters at HM GENERAL, Register House, 2 Princes Street, Edinburgh EH1 3YY, and

1.2.2. Local Authority Name (the Customer) having its headquarters at XXXXXXXXXXXX.

1.3. Terms of Agreement

1.3.1. The term of the Agreement, which covers the services specified in Section 2.1, will commence on <<date>>. The Agreement will be reviewed annually by the parties.

1.4. Obligations

1.4.1. The Provider will deliver the agreed services within the agreed timeframes, standards and costs, and in accordance with legal obligations which the Customer requires the Provider to meet.

1.4.2. Both parties agree to act in good faith and in a reasonable and timely manner with regard to the operation of the Agreement.

1.4.3. The parties agree to meet the costs, where material, of rework required as a result of their respective actions/errors following senior level consultation where appropriate.

1.5. Document Sign-Off and Security

1.5.1. The Agreement is to be signed by the Information Asset Owner (IAO) in duplicate and retained by both parties in a secure format. Electronic versions of the Agreement held by either party must also be kept in a secure format.
2. The Service

2.1. Services in Scope and Description

2.1.1. The Provider will provide the following services

a) **Advisory Service** relative to linkage, indexing and data in general, including information on the Provider’s data sets and associated variables where appropriate; the indexed file (data controllers ID and IndexID) and necessary information on the master indexing file (UID and IndexIDs); the overall quality of the data provided by the Customer to allow for provision of the Services by the Provider; and co-producing a set of access rules and protocols for the handling of Personal Data as part of the Service with the Customer and those across the broader Scottish Informatics and Linkage Collaboration (SILC). These rules and protocols will cover access to information and systems for the duration of this MoU, and may include procedures for the withdrawal of access and the return or deletion (at the Customer’s discretion) of all Personal Data on completion of the relevant Services and/or termination of this Agreement.

b) **Indexing Service** as part of the ‘separation of functions’ approach being used during the linkage process, in-line with the Data Linkage Framework and Scottish Informatics and Linkage Collaboration (SILC). This will include assigning a non-personal unique identifier (UID) to the Personal Data provided by the Customer via secure file transfer, together with such other information as the Provider may reasonably require in order to provide the Services; maintaining ‘look-up tables’ and ‘read-through’ which will allow for the development of more effective and efficient Service Provision; standard formatting of data before matching to ensure high quality accurate outputs as a result of the linkage being undertaken.

c) **Secure Data Transfer Service** as agreed with the Customer to allow for the secure transfer of Personal Data and attached non-personal UID’s between the Provider and the Customer; to securely transfer Index Keys to the Linkage Provider (NHS National Services Scotland or others as advised by the Customer).

3. Service Governance & Compliance

3.1. Governance Activities

3.1.1. The Provider and the Customer will operate under their established governance structures relative to their respective organisations. Additionally, both the Provider and the Customer will be governed in
relation to the processing of data by the Scottish Informatics and Linkage Centre – Strategic Management Board (SILC-SMB).

### 3.2. Compliance

3.2.1. As a minimum, the Provider shall comply in all respects and shall at all times act in such a manner to assist the Customer to comply, with the following:

- a) the Data Protection Act 1998 (DPA), and all codes and guidance issued pursuant thereto;
- b) the Human Rights Act 1998;
- d) the common law duty of confidentiality;
- e) the Scottish Government Identity Management and Privacy Principles;
- f) the Scottish Government’s Joined Up Data for Better Decisions Strategy;
- g) the Scottish Government’s Guiding Principles for Data Linkage; and
- h) The Scottish Government’s Security Classifications Policy and Handling Guidance in relation to:
  a. Transferring Personal Data securely
  b. Communication of personal data by: post, fax, phone, email and other electronic transfers of data;
  c. Storage of personal data on mobile devices including laptops, USB memory sticks, PDAs, Blackberries or any other mobile device or media such as smart phones, CD or DVD; and
  d. Anonymisation of data whenever feasible or appropriate;
- i) The Provider shall notify the Customer immediately if it becomes aware of any unauthorised or unlawful Processing, damage to or destruction of the Data, or if such Data becomes damaged, corrupted or unusable. The Provider shall follow the Procedure as detailed in Section 3.7.

### 3.3. Requirements

3.3.1. The Provider undertakes that it shall process the Personal Data strictly in accordance with the Customer’s instructions for the processing of that Personal Data.

3.3.2. The Provider will process the Personal Data for the purpose of providing the Services (Section 2.1).
3.3.3. The Customer will transfer the Personal Data in-line with the Government Security Classification Policy (Section 3.2).

3.3.4. The Provider agrees to inform the Customer as soon as possible (ideally within 3 working days) of all subject access requests which may be received from the Data Subjects. Where necessary the Provider will assist the Customer in processing the requests in line with the requirements of the DPA.

3.4. **Data**

3.4.1. The Customer shall provide the relevant Personal Data (see Section 3.6) to the Provider together with such other information as the Provider may reasonably require in order to provide the Indexing Service. All relevant Personal Data (see Section 3.6) will be transferred to the Provider in-line with the Customer’s security requirements.

3.4.2. The Customer shall provide only the minimum data necessary for the provision of the Services.

3.4.3. The instructions given by the Customer to the Provider in respect of the Personal Data shall at all times be in accordance with the laws of the United Kingdom.

3.5. **Privacy and Confidentiality**

3.5.1. The Provider will treat the Personal Data, and any other information provided by the Customer as confidential, and will ensure that access to the Contract Personal Data is limited to only those employees who require access to it for the purpose of the Provider carrying out the Services and complying with this Agreement and the Provider will ensure that all such employees have undergone training in the law of data protection, their duty of confidentiality under contract and in the care and handling of Personal Data.

3.5.2. The Provider will not disclose the Contract Personal Data to a third party under any circumstances other than at the specific written request of the customer, unless the disclosure is required by law.

3.6. **Personal Data**

3.6.1. The scope and type of Personal Data that may be provided to or accessed by the Provider as part of the Services consists of:-

- Local Authority Code;
- Approach reference (APPROACH_REF from PREVENT1)
- Application reference (APPREF from HL1);
- First Name
- Middle Name
- Last Name
• Date of Birth
• Gender
• Postcode (if known)

The full data specification and sample data are available at:

3.6.2. The Provider undertakes (on its own behalf and on behalf of the Customer) to treat all Personal Data in accordance with the provisions and principles of the DPA and to ensure only those of its staff who require to access Personal Data in the performance of their duties under this Agreement are able to do so, and that such staff are appropriately trained as a safe researcher and vetted to ensure their reliability.

3.6.3. The Provider shall only access Personal Data which is directly relevant to the effective execution by it of the terms of the Services.

3.6.4. The Provider will employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, alteration, transmission, publication, loss, destruction, theft or disclosure. Such technical and organisational measures will follow the Customer's Security Classification Policy and Handling Guidance (Section 3.2).

3.6.5. The Provider's organisational, operational and technological processes and procedures adopted are required to comply with the requirements of the UK HMG Security Policy Framework and UK HMG Information Security policies, guidelines and standards, including those produced by the CESG.

3.6.6. The Provider will not keep the Personal Data on any laptop or other removable drive or device unless that device is protected by being fully encrypted to the standards required under the Customer's Mobile Data Protection Standard available within the Scottish Government's Security Classifications Policy and Handling Guidance (Section 3.2) and the use of the device or laptop is necessary for the provision of the Services. Where this is necessary, the Provider will keep an audit trail of all such laptops, drives, and devices that Contract Personal Data is held on.

3.7. Loss of Data

3.7.1. The Provider shall notify the Customer immediately if it becomes aware of any loss of Personal Data. Following this, the Customer, as the Data Controller, will agree with the Provider the decisions to be taken and management of the incident. The Provider shall follow the Customer's Security Incident Reporting Policy by reporting, documenting and following up on all incidents, and reporting to senior management in both parties immediately. The outcome of any such investigation under the Security Incident Reporting Policy shall be notified to the Customer.
The Customer will support the Provider to meet these obligations as required.

3.8. **Ownership of Data**

3.8.1. All data remains the ownership of the Customer and other data controllers involved (either alone or jointly or in common with other persons). At no point will the Provider own the data.

3.8.2. The Provider will not sub-contract any of the Processing Activity or Data without the explicit written consent of the Customer. Where such consent is provided the Provider will ensure that any sub-Data Processor it uses to Process the Contract Personal Data enters into a written agreement which imposes the same obligations as are imposed on the Processor under this Agreement.

3.8.3. Where the sub-Data Processor fails to fulfil its obligations under any sub-Processing agreement, the Processor shall remain fully liable to the Customer for the fulfilment of its obligations under this Agreement.

3.9. **Intellectual Property Rights**

3.9.1. The Provider has no intellectual property rights pertaining to the processed data. All Intellectual Property Rights remain with the Customer and other data controller(s) involved (either alone or jointly or in common with other persons) unless stipulated elsewhere (for example in the project proposal).

3.10. **Records Retention**

3.10.1. All Personal Data shall be stored by securely by the Provider until such time as the outputs have been prepared for the Customer after which the Personal Data shall be destroyed securely in line with the data disposal policy standards for “OFFICIAL-SENSITIVE” information of the United Kingdom Government. The Provider must delete all records within 6 months of processing the data. However, read-through indexes may be retained until such point as the Customer instructs the Provider to delete them.

3.11. **Business Continuity**

3.11.1. To allow for business continuity, the Provider may, where appropriate and as agreed with the Customer, produce an index to allow for read-through to support efficient and effective linkage of future SILC projects.
3.12. **Audit Rights**

3.12.1. The Provider agrees that the Customer can, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks to ensure adherence to the terms of this MoU.

3.13. **Quality Assurance**

3.13.1. The Provider must take all reasonable measures to ensure the quality assurance of the processed data.

3.14. **Constraints**

3.14.1. The Provider must not, during and after the term of this Agreement:

   a) use any Contract Personal Data other than as directed by the Customer;

   b) use any Contract Personal Data for its own direct or indirect benefit, or the direct or indirect benefit of any third party, except that the Provider may use Contract Personal Data to the extent necessary to perform its duties and obligations, or to enforce its rights, under the Contract;

   c) allow Contract Personal Data to be accessed by, or sent to, parties outside the EEA (unless expressly required or permitted to do so by the Customer);

   d) seek to gain commercial advantage from its access to Contract Personal Data;

   e) disclose any Contract Personal Data to third parties, other than as required by the terms of this Agreement or as required by a court or other competent authority in which case the Customer and the Provider should discuss together the appropriate response to any and all such requests.

4. **Termination and Exit**

4.1. **Termination Rights**

4.1.1. Either party shall be entitled to terminate this Agreement by giving not less than 6 months written notice.

4.2. **Termination Process and Responsibilities**

4.2.1. Within 30 calendar days following termination of this Agreement by either party, the Provider shall, at the direction of the Customer:-
a) comply with any other agreement made between the parties concerning the return or destruction of Personal Data (Section 3.10);

b) return all Contract Personal Data passed to the Provider by the Customer; or

c) on receipt of instructions from the Customer, destroy all Contract Personal Data in its possession or control unless prohibited from doing so by any applicable law, and confirm in writing to the Customer that it has done so.

5. Charging and Payments

5.1. The Scottish Government has already provided payment for up to 30 projects which it has approved to be processed by “the Provider”. This MoU has been set-up to support delivery of these projects, with “the Provider” undertaking the processing of data as required to support the linkage in-line with the Data Linkage Framework, the Guiding Principles for Data Linkage and the broader Scottish Informatics and Linkage Collaboration (SILC) agenda.

5.2. There is no charge to Scottish Local Authorities for using this service.

6. Signatories

Service Customer:

Organisation: <<Local Authority Name>>

Name: Name of Head of Homelessness Service/ Information Asset Owner of Homelessness Data

Position: Head of Homelessness Service

Signature: ________________________ Date: __/___/___

Service Provider:

Organisation: National Records of Scotland (NRS)

Name: 

Position: 

Signature: ________________________ Date: __/___/___