
Data Controller/Data Processor Memorandum of
Understanding {MoU}
Service Requirements and Obligations
Between
The Scottish Government
and
Care Inspectorate

Contents

1. The Agreement.....	3
1.1. Statement of Intent.....	3
1.2. Parties to the Agreement.....	3
1.3. Terms of Agreement.....	3
1.4. Obligations.....	3
1.5. Document Sign-Off and Security.....	3
2. The Service.....	4
2.1. Services in Scope and Description.....	4
3. Service Governance & Compliance.....	4
3.1. Governance Activities.....	4
3.2. Compliance.....	4
3.3. Requirements.....	5
3.4. Data.....	5
3.5. Privacy and Confidentiality.....	5
3.6. Personal Data.....	5
3.7. Loss of Data.....	6
3.8. Ownership of Data.....	6
3.9. Intellectual Property Rights.....	6
3.10. Records Retention.....	7
3.12. Audit Rights.....	7
3.13. Quality Assurance.....	7
3.14. Constraints.....	7
4. Termination and Exit.....	8
4.1. Termination Rights.....	8
4.2. Termination Process and Responsibilities.....	8
5. Signatories.....	8

The Agreement

1.1. *Statement of Intent*

- 1.1.1. This document ("the Agreement") is a memorandum of understanding between the Care Inspectorate ("the Provider") and the Scottish Government ("the Customer") in relation to the provision of data processing 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 Care Inspectorate (the Provider) having its headquarters at Compass House, 11 Riverside Drive, Dundee, 001 4NY
- 1.2.2. ~~The Scottish Government (the Customer)~~ having its headquarters at St Andrew's House, Regent Road, Edinburgh. EH1 3DG

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 01 Feb 2017. The Agreement will be reviewed annually by the parties at the completion of each census.

1.4. *Obligations*

- 1.4.1. The Provider will deliver the agreed services set out in section 2.1 within the agreed timeframes and standards, and in accordance with legal obligations which the Customer requires the Provider to meet as set out in Clause 3 hereof.
- 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) **Data Collection** of the annual Scottish Care Homes Census. Collection of data through the Care Inspectorate eForm system and customer support to Care Homes provided through the Helpdesk.
- b) The dataset will be used to pre-populate the Scottish Care Home Census eform for the following census year. The dataset is used for 'statistics and research purposes' only.
- c) The dataset will be securely transferred to the customer following completion of data collection, using a method agreed with 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.

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;
- c) The Freedom of Information (Scotland) Act 2002 and Environmental Information (Scotland) Regulations 2004
- d) the common law duty of confidentiality;
- e) the Scottish Government Identity Management and Privacy Principles;

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 Provider will transfer the Personal Data in-line with the specific instructions of the Provider.
- 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 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 collected by the Provider as part of the Services consists of:-
 - name;
 - date of birth;
 - postcode;
 - gender;
 - ethnicity;
 - disability / health condition

- 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.
- 3.6.3. The Provider shall only collect & process Personal Data for the purposes of this Agreement 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.
- 3.6.5. 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 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 Contain 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 in the management of the incident. The Provider shall follow the Customer's **Security Incident Reporting Policy** (Annex A) by reporting, documenting and following up on all incidents, and reporting to senior management in both parties immediately. The outcome of any security 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 collected solely for the purposes of providing the services remains in 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 such 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.

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 securely by the Provider and may be retained until such point as the Customer instructs the Provider to delete them. Data must be retained for at least one year in order to pre-populate the following years form in order to ease the burden on data providers.

3.11. 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.

3.12. Quality Assurance

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

3.13. Constraints

- 3.13.1. 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.

*Contract Personal Data refers to the personal data collected as part of the Scottish Care Homes Census set out in section 3.6.

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.

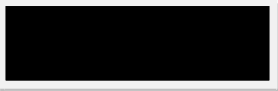
5. Signatories

Service Customer:

Organisation: Scottish Government, Health and Social Care Analysis

Name: Angela Campbell

Position: Deputy Director, Health and Social Care Analysis


Signature  Date: 17/02/17

Service Provider.

Organisation: Care Inspectorate

Name: Karen Reid

Position: Chief Executive, Care Inspectorate

Signature:  Date: 31/01/17

Annex A: Security Incident Reporting

Definition (taken from Scottish Government Intranet on 16/01/2017):

A security incident may be defined as any event which deviates from the SG's security policies and procedures and does not have the approval of the officer authorised to agree such deviation. Such events will result in the SG, individuals, ICT systems and/or the information held on them being exposed, or potentially exposed, to illegitimate access. As a result, incidents have the potential to compromise SG business, the Data Protection Act as well as the Confidentiality, Integrity and/or Availability of ICT systems and/or the information that is held on them.

Incidents can cover a wide range of events and may be categorised as below:

- Physical: the loss of hard copy personal/sensitive/protectively marked material, the breaching of access controls (including lost/stolen security passes); the loss/theft of personal/sensitive/protectively marked data or equipment; unauthorised access to, tampering with or use of ICT systems, equipment or accounts; unauthorised acquisition of privileges; unauthorised access to, use or disclosure of sensitive information; unauthorised changes to system hardware, firmware or software; suspect packages and bomb threats.
- Procedural: improper use of an ICT system, access or privileges (e.g. inappropriate use of email or accessing inappropriate web sites); improper handling, distribution, accounting, storage and destruction of cryptographic items or sensitive information;
- Personnel: any unauthorised event involving insiders or ex-insiders (including members of staff, contractors, visitors, support staff or former members of any of these groups);
- Electronic: malware attacks (viruses, worms, Trojan horses); unauthorised disruption of service (denial of service and distributed denial of service attacks), receipt of spam, phishing attacks, etc.;
- Operational: system failures, crashes, environmental failures and operator errors may have security implications and should be treated as incidents, in addition to their potential implications for business continuity. Some IT security incidents have been detected as a result of poorer system performance being detected.

The examples given above are not exhaustive and many incidents will belong to more than one category. Other incidents may be difficult to classify so we have to be alert to the possibility of new types or manifestations of incident, particularly as attack methods are constantly evolving.

Reporting a security incident

To report a security incident, the attached Security Incident Report Form must be completed by the individual responsible for the incident or by the person who first dealt with it or became aware of the incident. Part 2 must be completed by an individual in the line management chain. On completion, the form must be submitted to the Office of Protective Security mailbox.

0037375.docx

If the incident involves the loss of information, the matter must be reported immediately. If it occurs outside of office hours, the Security Control Room must be contacted on 0131 244 5203. On receipt of your call, the duty officer from the Office of Protective Security will be notified and will contact you to discuss the incident further.