

CONTRACT REFERENCE NUMBER: 17/01/54

SERVICES CONTRACT

-between-

**(1) THE REGISTRAR GENERAL OF BIRTHS, DEATHS AND MARRIAGES FOR SCOTLAND
(THE "AUTHORITY")**



-and-

(2) CACI LIMITED (THE "SERVICE PROVIDER")

CACI

-relating to the supply of-

SERVICES FOR

THE PROVISION OF AN ONLINE COLLECTION INSTRUMENT FOR SCOTLAND'S CENSUS 2021



SCHEDULE 9

MODEL TERMS FOR DATA PROTECTION DIRECTIVE 95/46/EC

This and the five (5) following pages comprise Schedule 9 referred to in the foregoing Services Contract between the Registrar General of Births Deaths and Marriages for Scotland and CACI Limited

SCHEDULE 9 – DATA PROTECTION

Part 1: Data Processing provision as required by Article 28(3) GDPR.

This Part includes certain details of the Processing of Personal Data in connection with the Services:

- 1.1.1 Subject matter and duration of the Processing of Personal Data
- 1.1.2 The subject matter and duration of the Processing of Personal Data are set out in the Contract.
- 1.1.3 The nature and purpose of the Processing of Personal Data
- 1.1.4 Online Collection Instrument for Scotland's Census 2021 Contract (17/01/54)
- 1.1.5 The types of Personal Data to be Processed
- 1.1.6 Census Data and Authority Data
- 1.1.7 The categories of Data Subject to whom Personal Data relates
- 1.1.8 The obligations and rights of the Purchaser

The obligations and rights of the Purchaser as the Data Controller are set out in Clause 14 of the Contract.

Part 2

Model Contract

**STANDARD FORM CONTRACT TO ASSIST COMPLIANCE WITH OBLIGATIONS IMPOSED BY
ARTICLE 17 OF THE DATA PROTECTION DIRECTIVE 95/46/EC**

**(FOR USE BY DATA CONTROLLERS AND DATA PROCESSORS LOCATED WITHIN THE EUROPEAN
ECONOMIC AREA WHERE THE PARTIES HAVE ENTERED INTO A SEPARATE DATA PROCESSING
AGREEMENT)**

THIS AGREEMENT is made on 1 February 2018.

BETWEEN:

(1) THE REGISTRAR GENERAL OF BIRTHS, DEATHS AND MARRIAGES FOR SCOTLAND (the "Controller"); and

(2) CACI LIMITED. Registered in England & Wales. Registration No. 1649776 whose registered office is at CACI House, Avonmore Road, London, W14 8TS (the "Processor").

BACKGROUND

- (A) The Controller processes Personal Data in connection with its business activities;
- (B) The Processor processes Personal Data on behalf of other businesses and organisations;
- (C) The Controller wishes to engage the services of the Processor to process personal data on its behalf in relation to [drafting note: insert scheme name];
- (D) Article 17(2) of the Data Protection Directive 95/46/EC (as hereinafter defined) provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;
- (E) Articles 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a processor on behalf of a controller such processing shall be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;
- (F) In compliance with the above-mentioned provisions of Article 17 of the Data Protection Directive the Controller and Processor wish to enter into this processing security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"**Data Protection Directive**" shall mean Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"**national law**" shall mean the law of the Member State in which the Processor is established;

"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"sub-contract" and **"sub-contracting"** shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and **"Sub Contractor"** shall mean the party to whom the obligations are subcontracted; and

"Technical and organisational security measures" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing.

2. CONSIDERATION

2.1 In consideration of the Controller engaging the services of the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

3. SECURITY OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall only carry out those actions in respect of the personal data processed on behalf of the Controller as are expressly authorised by the Controller.

3.2 The Processor shall take such Technical and Organisational Security Measures as are required under its own national law to protect personal data processed by the Processor on behalf of the Controller against unlawful forms of processing. Such Technical and Organisational measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 1 of this Agreement.

4. CONFIDENTIALITY

4.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, save with the prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

4.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of services by the Processor to the Controller.

4.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

5. SUB-CONTRACTING

5.1 The Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Controller.

5.2 Where the Processor, with the consent of the Controller, sub-contracts its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Processor under this Agreement.

- 5.3** For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub-processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement

6. TERM AND TERMINATION

- 6.1** This Agreement shall continue in full force and effect for so long as the Processor is processing personal data on behalf of the Controller.
- 6.2** Within 28 days following termination of this Agreement the Processor shall, at the direction of the Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data, or (b) return all personal data passed to the Processor by the Controller for processing, or (c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

7. GOVERNING LAW

- 7.1** This Agreement shall be governed by and construed in accordance with the national law of the Member state in which the Controller is established.

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [CONTROLLER]

(Authorised signatory)

(Print name and title) Tim Ellis, Registrar General of Births Deaths and Marriages for Scotland

SIGNED on behalf of [PROCESSOR]

(Authorised signatory)

(Print name and title) Greg Bradford, Chief Executive

APPENDIX 1¹

1. Legal requirements

1.1 The Processor shall, in respect of the processing of personal data on behalf of the Controller, identify and comply with any specific security provisions imposed by its national law.

2. Practical security measures

2.1 In compliance with its obligations under clause 3.2 with regard to the processing of personal data on behalf of the Controller, the Processor, as a minimum requirement, shall give due consideration to the following types of security measures:

2.1.1 Information Security Management Systems;

2.1.2 Physical Security;

2.1.3 Access Control;

2.1.4 Security and Privacy Enhancing Technologies;

2.1.5 Awareness, training and security checks in relation to personnel;

2.1.6 Incident/Response Management/Business Continuity; and

2.1.7 Audit Controls/Due Diligence;

Signature

Signature

¹ The Practical Security Measures outlined in Schedule 1 are taken from the OECD Working Party on Information Security and Privacy's draft paper of 30-31 March 2004 entitled "Information Security Issues and Resources for Small and Entrepreneurial Companies – A business companion to the 2002 OECD Guidelines for the Security of Networks and Information systems: Towards a Culture of Security"