Registers of Scotland
ros.gov.uk

REGISTERS OF SCOTLAND CONDITIONS OF CONTRACT

SCHEDULE

DATA PROTECTION

1. Definitions

1.1 **Data Subject Access Request**: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

Sub-processor: any third party appointed to process Personal Data on behalf of the Supplier in connection with this Contract

1.2 **"Controller" , "Processor" , "Data Subject" , "Personal Data" , "Personal Data Breach" , "Data Protection Officer** " shall have the meanings assigned to them in the GDPR.

2 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Purchaser is the Controller and the Supplier is the Processor. The only processing that the Supplier is authorised to do is listed in Annex A to this Schedule which sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of personal data. The Supplier shall notify the Purchaser immediately if it considers that any of the Purchaser's instructions infringe the Data Protection Legislation.

3 Both Parties agree to negotiate in good faith any such amendments to this Contract that may be required to ensure that both Parties meet all their obligations under Data Protection Legislation. The provisions of this paragraph 3 are without prejudice to any obligations and duties imposed directly on the Supplier under Data Protection Legislation and the Supplier hereby agrees to comply with those obligations and duties.

4 The Supplier will, in conjunction with the Purchaser and in its own right and in respect of the Services, make all necessary preparations to ensure it will be compliant with Data Protection Legislation.

5 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

5.1 process that Personal Data only as necessary and in accordance with Annex A to this Schedule, unless the Supplier is required to do otherwise by Law; in which case the Supplier shall promptly notify the Purchaser before processing the Personal Data unless prohibited by Law;

5.2 ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it, having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from unauthorised or unlawful processing of, or accidental loss, destruction or damage to, Personal Data;

(iii) state of technological development; and

(iv) cost of implementing any measures;

5.3 ensure that it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Supplier's duties under this clause;

(ii) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Purchaser or as otherwise permitted by this Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data;

5.4 not transfer Personal Data outside of the European Economic Area unless the prior written consent of the Purchaser has been obtained and the following conditions are fulfilled:

(i) the Purchaser or the Supplier has provided appropriate safeguards in relation to the transfer;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(iv) the Supplier complies with reasonable instructions notified to it in advance by the Purchaser with respect to the processing of the Personal Data;

6 Taking into account the nature of the processing the Supplier must provide full assistance to the Purchaser in relation to the Purchaser's obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations. Without prejudice to the foregoing generality, the Supplier shall:

6.1 notify the Purchaser immediately if receives a Data Subject Access Request or any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation and provide such assistance as is reasonably requested by the Purchaser to enable the Purchaser to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation

6.2 notify a Personal Data breach to the Purchaser without undue delay and in any event no later than 24 hours after becoming aware of a Personal Data breach and assist the Purchaser with communication of a personal data breach to a Data Subject;

6.3 support the Purchaser with preparation of a data protection impact assessment;

6.4 provide assistance as requested by the Purchaser with respect to any request from the Information Commissioner's Office, or any consultation by the Purchaser with the Information Commissioner's Office.

7 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

(i) the Purchaser determines that the processing is not occasional;

(ii) the Purchaser determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(III) the Purchaser determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

8 The Supplier shall allow for audits of its Data Processing activity by the Purchaser or the Purchaser's designated auditor.

9 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

10 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Supplier must:

(i) notify the Purchaser in writing of the intended Sub-processor and processing;

(ii) obtain the written consent of the Purchaser;

(iii) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Schedule such that they apply to the Sub-processor;

(iv) provide the Purchaser with such information regarding the Sub-processor as the Purchaser may reasonably require

11 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

12 At the end of the provision of the Services the Supplier must, on written instruction of the Purchaser, delete or return to the Purchaser all Personal Data and delete existing copies unless the Supplier is required by Law to retain the Personal Data.

ANNEX A

1 The Supplier shall comply with any further written instructions with respect to processing by the Purchaser

2. Any such further instructions shall be incorporated into this Annex A.

Description	Details
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*
Nature and purposes of the processing	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
Plan for return and destruction of the data once the processing is complete (unless a requirement under union or member state law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*