CROWN COMMERCIAL SERVICE

AND

SUPPLIER

WORKPLACE SERVICES CONTRACT

(FM MARKETPLACE PHASE 2)

REF: RM6089

PROCESSING DATA

1. Only the Relevant Authority can decide what processing of Personal Data a Supplier can do under a Contract and must specify it for each Contract using the template in Annex 1 (Authorised Processing) to this Schedule.

2. The Supplier must only process Personal Data if authorised to do so in Annex 1 (Authorised Processing) by the Relevant Authority. Any further written instructions relating to the processing of Personal Data are incorporated into Annex 1 to this Schedule.

3. The Supplier must give all reasonable assistance to the Relevant Authority in the preparation of any Data Protection Impact Assessment before starting any processing, including:

- a systematic description of the expected processing and its purpose
- the necessity and proportionality of the processing operations
- the risks to the rights and freedoms of Data Subjects
- the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data

4. The Supplier must notify the Relevant Authority immediately if it thinks the Relevant Authority's instructions breach the Data Protection Legislation.

5. The Supplier must put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Relevant Authority.

6. If lawful to notify the Relevant Authority, the Supplier must notify it if the Supplier is required to process Personal Data by Law promptly and before processing it.

7. The Supplier must take all reasonable steps to ensure the reliability and integrity of any Supplier Staff who have access to the Personal Data and ensure that they:

- are aware of and comply with the Supplier's duties under this Schedule;
- are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
- are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Relevant Authority or as otherwise allowed by the Contract;
- have undergone adequate training in the use, care, protection and handling of Personal Data.

8. The Supplier must not transfer Personal Data outside of the EU unless all of the following are true:

- it has obtained prior written consent of the Relevant Authority;
- the Relevant Authority has decided that there are appropriate safeguards as referenced under GDPR Article 46;
- the Data Subject has enforceable rights and effective legal remedies when transferred;
- the Supplier meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred;
- where the Supplier is not bound by Data Protection Legislation it must use its best endeavours to help the Relevant Authority meet its own obligations under Data Protection Legislation;
- the Supplier complies with the Relevant Authority's reasonable prior instructions about the processing of the Personal Data.

9. The Supplier must notify the Relevant Authority immediately if it:

- receives a Data Subject Access Request (or purported Data Subject Access Request);
- receives a request to rectify, block or erase any Personal Data;
- receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
- receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law;
- becomes aware of a Data Loss Event.

10. Any requirement to notify under Paragraph 9 includes the provision of further information to the Relevant Authority in stages as details become available.

11. The Supplier must promptly provide the Relevant Authority with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 9. This includes giving the Relevant Authority:

- full details and copies of the complaint, communication or request;
- reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
- any Personal Data it holds in relation to a Data Subject on request;
- assistance that it requests following any Data Loss Event;
- assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office.

12. The Supplier must maintain full, accurate records and information to show it complies with this Schedule. This requirement does not apply where the Supplier employs fewer than 250 staff, unless either the Relevant Authority determines that the processing:

- is not occasional;
- 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;
- is likely to result in a risk to the rights and freedoms of Data Subjects.

13. The Supplier must appoint a Data Protection Officer responsible for observing its obligations in this Schedule and give CCS and each Buyer their contact details.

14. Before allowing any Sub-processor to process any Personal Data, the Supplier must:

- notify the Relevant Authority in writing of the intended Sub-processor and processing
- obtain the written consent of the Relevant Authority
- enter into a written contract with the Sub-processor so that this Schedule applies to the Sub-processor
- provide the Relevant Authority with any information about the Sub-processor that the Relevant Authority reasonably requires

15. The Supplier remains fully liable for all acts or omissions of any Sub-processor.

16. At any time the Relevant Authority can, with 30 Working Days' notice to the Supplier, change this Schedule to:

- replace it with any applicable standard clauses (between the controller and processor) or similar terms forming part of an applicable certification scheme under GDPR Article 42.
- ensure it complies with guidance issued by the Information Commissioner's Office (being the independent body set up in the United Kingdom with the primary purpose to uphold information rights in the public interest, www.ICO.org.uk).

17. The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner's Office.

ANNEX 1

AUTHORISED PROCESSING

Call-Off Contract(s): **TBC**	**Framework RM 6089 Lot 2A**
Date: 23 June 2021	
Description of Authorised Processing	**Details**
Subject matter of the processing	The personal data of the Occupant of an SFA, or carer/guardian/representative (neighbour)/etc. who will be present at an appointment to carry out an inspection of the SFA + personal data of any vulnerable adults / dependants. The personal data of a prospective Occupant of an SFA and, or carer/guardian/representative, who will be present at an appointment to view an SFA prior to occupation + personal data of any vulnerable adults / dependants.
Duration of the processing	The processing could occur at any time during the duration of the Contract.
Nature and purposes of the processing	To facilitate setting up and attending an appointment to undertake a housing inspection. To facilitate setting up and attending an appointment for a potential Occupant to view an SFA prior to occupation. To manage the appointment and record the outcome of the appointment. To meet any reporting requirements – only where required this to include Occupant endorsement of any findings from an inspection optional satisfaction survey / complaint / notes against future appointment associated with the same task.
Type of Personal Data	Occupant or carer/guardian/representative (neighbour) name and contact details (telephone number or other Occupant, carer/guardian/representative favoured means of communication).

	Occupant special requirements/vulnerabilities needed to support the provision of the Service but EXCLUDING any medical data.
Categories of Data Subject	Occupant or carer/guardian/representative. Family/dependant(s). Vulnerable adult/dependant(s) details.
Other Call-Off Contract Specific Requirements (in accordance with Clause 2 of this Schedule)	1. For the avoidance of doubt, for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor. 2. The Protective Measures put in place by the Supplier must take into account, as a minimum, the: • nature of the data to be protected; • harm that might result from a Data Loss Event; • state of technological development; and • cost of implementing any measures. 3. In addition to clause 7 of this Schedule, the Supplier must ensure all Supplier Staff who have access to the Personal Data must have the necessary probity by undertaking the Baseline Personnel Security Standard or standard as specified in this Call-Off Contract. 4. The Supplier shall allow for audits of its Data Processing activity by the Buyer or the Buyer's designated auditor as required to demonstrate the Buyer's compliance with its obligations as a Controller. Such audits will be conducted in accordance with general audit conditions contained in the Call-Off Contract. 5. At the written direction of the Buyer, the Supplier shall delete or return Personal Data (and any copies of it) to the Authority on termination of the Contract unless the Buyer is required by Law to retain the Personal Data.