**Variation to G-Cloud 11 Call-Off** (RM1557.11)

Call-Off Contract reference - 00576317

Call-Off Contract title - Government Shared Services Kahootz Licences

Between Government Shared Services (“the Buyer”)

And INOVEM Limited (trading as Kahootz) (“the Supplier”)

1. This Call Off Contract is varied as follows and shall take effect on the date signed by both Parties:
	1. **The Call-Off Contract value** shall be increased from £65,197 to £81,317
	2. **The GCloud Services Required** shall be removed and replaced with the following:

REDACTED

* 1. **Invoice frequency** shall be updated to:
		1. REDACTED
	2. **Call-Off Contract Charges shall be updated to:**
		+ 1. REDACTED
	3. Additional Buyer Terms - Personal Data and Data Subjects shall be updated to:
		1. Annex 1 of Schedule 7 is being used, The Cabinet Office is the Controller for and the Supplier is the Processor.
	4. **Schedule 7 - GDPR information** shall be updated to reflect the amendments in Annex A to this Variation.
1. Words and expressions in this Variation shall have the same meanings given to them in this Call Off Contract.
2. This Call Off Contractshall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory on behalf of the Buyer

**Signature REDACTED**

**Date** 26/6/2020

**Name**

**Title**

Signed by an authorised signatory on behalf of the Supplier

**Signature REDACTED**

**Date** 24/06/2020

**Name**

**Title**

**Annex A**

# Schedule 7 - GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

## Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer’s Data Protection Officer are: REDACTED

1.2 The contact details of the Supplier’s Data Protection Officer are: REDACTED

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description**  | **Details**  |
| Identity of Controller for each Category of Personal Data  | **The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of all personal Data.  |
| Duration of the Processing  | *Names and email addresses for users will be retained for the duration of their account use. Users comments or questions on forums which display their name will be held as long as the site is in use.* *Board papers with names will only be stored for 1 year.* *For the duration of the contract with Kahootz.*  |

|  |  |
| --- | --- |
| Nature and purposes of the Processing  | *Processing includes personal data collection for account creation and use and consultation e.g. feedback forms and forums where name/email address is provided.* *Kahootz is used for sharing information such as documents, templates and review records etc, where a common platform doesn’t exist. This allows users to collaborate and share information easily.* *For example, the IPA organise, manage and provide assurance reviews on government major programmes and projects, as well as EU Transition and COVID related reviews. Most reviews include a combination of document review and stakeholder interviews. Kahootz will be used as a x-govt document and collaboration space to support assurance reviewers.*  |
| Type of Personal Data  | * *Name and email address are processed to set up a Kahootz account*
* *We will process the following personal data in relation to user accounts: name, email address, job title, employer, activity on the platform.*
* *Names are included in ‘attendees’ for Board papers, access to these papers is locked down to Board members and is not publicly visible*
* *Names are included in Action trackers for projects shared between SSCL, GSS and Fujitsu*
* *Names are displayed if individuals choose to comment or engage in a forum available in Kahootz, this can also be done anonymously*
* *An email address would be supplied if a user submitted a feedback form to the site owner in OneGovCloud*
* A phone number without name is provided in the ‘contact us’ section of the OneGovCloud Kahootz site
* *We will process the following personal data in relation to programme documents shared on the platform: name, email address, job title, employer, phone numbers and opinions.*

 |
| Categories of Data Subject  | * Civil servants
* SSCL staff working on specific projects
* Fujitsu staff working on specific projects

 |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data  | *When kahootz workspaces are no longer in use they will be deleted by the controller. When a user no longer needs access to kahootz the controller will remove them.* *At the end of the contract the processor will delete all customer data.*  |

### 2. Undertakings of Both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

1. report to the other Party every 3 months on:
	* 1. the volume of Data Subject Request (or purported Data Subject

Requests) from Data Subjects (or third parties on their behalf);

* + 1. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
		2. any other requests, complaints or communications from Data

Subjects (or third parties on their behalf) relating to the other Party’s obligations under applicable Data Protection Legislation;

* + 1. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
		2. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

1. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
2. provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
3. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex.
4. request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
5. ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
6. take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
	1. are aware of and comply with their ’s duties under this Annex 2

(Joint Controller Agreement) and those in respect of Confidential Information

* 1. are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;
	2. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
1. ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
2. nature of the data to be protected;
	1. harm that might result from a Data Loss Event;
	2. state of technological development; and
	3. cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other

Controller to comply with any obligations under applicable Data Protection

Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

### 3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

1. sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;
2. all reasonable assistance, including:
	* 1. co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
		2. co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
		3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
		4. providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data

Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party’s own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

* + - 1. the nature of the Personal Data Breach;
			2. the nature of Personal Data affected;
			3. the categories and number of Data Subjects concerned;
			4. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
			5. measures taken or proposed to be taken to address the Personal Data Breach; and
			6. describe the likely consequences of the Personal Data Breach.

### 4. Audit

4.1 The Supplier shall permit: (a) the Buyer, or a third-party auditor acting under the Buyer’s direction, to conduct, at the Buyer’s cost, data privacy and security audits, assessments and inspections concerning the Supplier’s data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer’s direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier’s compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

### 5. Impact Assessments

5.1 The Parties shall:

1. provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

1. maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

### 6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days’ notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

### 7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

1. if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

1. if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

1. if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).
	1. If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“Court”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
	2. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):
2. if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

1. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

1. if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

### 9. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2

(*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 18.5 (*Ending the contract*).

### 10. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

1. carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
2. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

### 11. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.