

**ANNEX E****Form for Direct Award and Award Following a Further Competition****ORDER FORM****SECTION A**

This Order Form is issued in accordance with the provisions of the Internal Audit Services for the Government Internal Audit Agency Framework Agreement (RM 4167). The Supplier agrees to supply the Services specified below on and subject to the terms of this Call Off Contract and for the avoidance of doubt this Call Off Contract consists of the terms set out in this Order Form and the Call Off Terms.

**DATE** 06/02/2018

**ORDER NUMBER** RM4167/GIAA/KPMG/2019/

**FROM**

Mike Barrett, Deputy Head of Internal Audit, 100 Parliament St,  
London SW1A2BQ, Tel: 07718159228 "**CUSTOMER**"

**TO**

**KPMG, 15 Canada Square, Canary Wharf, London "SUPPLIER"**

**SECTION B****1. CALL OFF CONTRACT PERIOD****1.1 Call Off Commencement Date:**

January 2019

**1.2 Call Off Expiry Date:**

End date of Call Off Initial Period

March 31, 2019

End date of Call Off Extension Period

To be defined at a later date, as required.

**2. CUSTOMER CORE SERVICES REQUIREMENTS****2.1 Services required**

The services required are:

The Data Analytics project has been commissioned by Internal Audit following a CFO leadership event that was held on 12 April 2018. The project aims to provide the foundation for introducing data analytics capability within Internal Audit and a longer term aim of passing tools over to the first and second lines of defence in the Business.

In line with the approved project plan, the Project Team has agreed for the Cash Management and Payroll audits on the 2018/19 audit plan to be used as a proof of concept for data analytics.

The scope of work of the Cash Management audit primarily involves performing data analytics routines over HMRC's Cash Flow management processes that enable Corporate Treasury to fund business activities, process payment of taxes, duties and benefits and administering HMRC's bank accounts effectively, enabling payments to be made and receipts to be transferred to the Bank of England.

The work to be performed would include coverage of the following data analytics routines:

#### Master Data

- Changes to bank accounts (can-do and did-do) Comparison of bank accounts to HR master data Temporary/multiple changes to bank accounts Authorisation of changes to bank accounts. Opening and closing of bank accounts Accounts no longer used Accounts not in approved list

#### Transactional

- Transactions stuck in SAP
- Duplicate transactions
- Manual activity
- Trend analysis
- Bank account transfers
- Cash journal postings
- User Segregation of Duties analysis

The scope of work of the Payroll audit is to test the integrity of the payroll system and quality of data.

The work to be performed would include coverage of the following areas:

- Review of salaries using data analytics tools and techniques- analyses to include duplicate salary payments, payments to non-employees, overtime and leave;
- Performance of data analytics routines over HMRC salary and HR data for 100% of employees in the SAP system to provide outputs in the form of reports which will highlight exceptions or anomalies which can then be investigated for deviation from policy.
- Confirmation that access to payroll systems is restricted with appropriate levels of segregation of duties.
- Extraction and processing of relevant data to generate the outputs for the analyses agreed plus additional routines such as; analysis of average by role/grade to identify outliers, analysis of average salary by geographical location, and breakdown of "additional" payments.

A detailed analytics work programme will be prepared and agreed following an initial scoping phase covering these areas.

The specific systems to be included in scope will be agreed following the scoping phase.

#### **Output:**

Documents providing content for the Cash Management and Payroll audit reports. This will include:

- All findings and identified discrepancies.
- Provision of solutions to remediate discrepancies identified.
- Input into the level of assurance to be provided in the audit report.
- A list of identified users with segregation of duties conflicts.

**2.2 NOT USED**

**2.3 NOT USED**

**2.4 NOT USED**

**2.5 Location/Sites of Delivery**

KPMG will use a secure server provided by HMRC in Worthing. This has been agreed by CDIO and Security. It will be an HMRC server without any connectivity with the outside world. It will be housed in an HMRC secure room and the data will be deleted after use by HMRC security.

**2.6 Dates for Delivery of the Services**

As required by customer within Call off period

**2.7 Implementation Plan**

This section 2.7 replaces Schedule 4 of the Call Off Terms.

**2.8 Standards**

The Supplier shall comply with Clause 11 (STANDARDS AND QUALITY) of the Call Off Terms.

**2.9 Service Levels**

The Supplier shall conform to Part A of Schedule 6 (Service Levels and Performance Monitoring) of the Call Off Terms.

**2.10 Not Used**

**2.11 Business Continuity and Disaster Recovery (Schedule 9)**

**Not Used**

**2.12 Performance Monitoring**

[As per Annex 1 to Part B (Additional Performance Monitoring Requirements) of Call Off Schedule 6 (Service Levels and Performance Monitoring),

**2.13 Security**

The Supplier shall conform to Call Off Schedule 8 (Security), 'SHORT FORM'.  
SC required and vetting certificates provided

#### **2.14 Period for providing the Rectification Plan**

5 Working Days

#### **2.15 Exit Management (Schedule 10)**

**Not Used**

### **3. SUPPLIER'S INFORMATION**

#### **3.1 Supplier's inspection of Sites, Customer Property and Customer Assets**

Not Used

#### **3.2 Commercially Sensitive Information**

All information viewed or extracted must be held secure at all times and not left unattended. Any papers, documents, emails with information relating to the documents sent should be deleted or destroyed on completion of the audit work. All documents classified as Official Sensitive are exchanged via gsi email accounts, with prior approval from Internal Audit.

### **4. CUSTOMER RESPONSIBILITIES**

#### **4.1 Customer Responsibilities**

As per Part B of Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key Personnel)

This section 4.1 replaces Part B of Schedule 4 of the Call Off Terms.

### **5. CALL OFF CONTRACT CHARGES AND PAYMENT**

#### **5.1 Call Off Contract Charges payable by the Customer (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile including method of payment (e.g. Government Procurement Card (GPC) or BACS)**

As per Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)

The resource required for the Cash Management audit will be based on the KPMG Data Analytic proposal dated 14 December 2018 with the estimated budget and costs not to exceed the original estimate of £21,000 plus expenses which will be charged at cost.

No of days required – 10 days

Level of staff required – Director, Senior Manager and Manager

The resource required for the Payroll Audit will be based on the original KPMG Data Analytic proposal dated 26 June with the estimated budget and costs not to exceed the original estimate of £25,000 plus expenses which will be charged at cost.

Send Invoices and Payments Requests to:

Mail : Financial Shared Services

Accounts Payable

B Spur, South Block

Barrington Road

Worthing

West Sussex

BN12 4XH

Email : [payments.team@hmrc.gsi.gov.uk](mailto:payments.team@hmrc.gsi.gov.uk)

Invoices emailed to Accounts Payable can only be accepted in PDF format which is non changeable.

Any invoices sent in a changeable form such as: spreadsheets (xls) Word documents (doc) or Pictures (bmp/jpg) cannot be acceptable electronically and must be submitted to Accounts Payable in paper format. The preference towards PDF invoicing is a reflection of the Corporate Finance commitment towards reducing the amount of paper invoices received.

If an invoice is overdue or urgent payment is required a copy of the invoice can be e-mailed to Accounts Payable. The invoice must be marked as 'Certified and True Copy' and accompanied by an explanatory note for audit purposes.

In the interest of avoiding duplications, the Accounts Payable will not process statements. If a vendor has only supplied a statement to you please contact them and ask for a full VAT invoice.

Invoices emailed to Accounts Payable can only be accepted in PDF format which is non changeable.

Any invoices sent in a changeable form such as: spreadsheets (xls) Word documents (doc) or Pictures (bmp/jpg) cannot be acceptable electronically and must be submitted to Accounts Payable in paper format. The preference towards PDF invoicing is a reflection of the Corporate Finance commitment towards reducing the amount of paper invoices received.

If an invoice is overdue or urgent payment is required a copy of the invoice can be e-mailed to Accounts Payable. The invoice must be marked as 'Certified and True Copy' and accompanied by an explanatory note for audit purposes.

In the interest of avoiding duplications, the Accounts Payable will not process statements. If a vendor has only supplied a statement to you please contact them and ask for a full VAT invoice.

## **5.2 Estimated Year 1 Call Off Contract Charges**

As above for period stated

## **5.3 Undisputed Sums Limit**

For the purposes of Clause 42.1.1 the Undisputed Sums Limit

This section 5 replaces Annexes 1 and 2 of Schedule 3.

The Supplier shall submit invoices directly to

<mailto:mike.j.barrett@hmrc.gsi.gov.uk>

## **SECTION C**

### **6. CUSTOMER OTHER CONTRACTUAL REQUIREMENTS**

#### **6.1 Call Off Guarantee**

Not used

#### **6.2 Key Personnel**

HMRC <mailto:mike.j.barrett@hmrc.gsi.gov.uk>

KPMG: [\[mailto:andrew.c.north@kpmg.co.uk\]](mailto:andrew.c.north@kpmg.co.uk)

#### **6.3 Relevant Convictions**

Clause 27.2.1 of the Call Off Terms shall apply.

#### **6.4 Failure of Supplier Equipment**

Not used

#### **6.5 Protection of Customer Data**

Not used

#### **6.6 Testing**

Not used. Clause 12 and Schedule 5 are therefore deleted.

#### **6.7 Limitations on Liability**

Clause 36 (LIABILITY) of the Call Off Terms shall apply.

#### **6.8 Insurance**

Clause 37 (INSURANCE) of the Call Off Terms shall apply.

#### **6.9 Termination without cause notice period**

The minimum number of days for the purposes of Clause 41.7 (TERMINATION WITHOUT CAUSE) of the Call Off Terms shall be ten (10)



## 7. ADDITIONAL AND/OR ALTERNATIVE CLAUSES

### 7.1 Supplemental requirements to the Call Off Terms

#### **1 PROTECTION OF PERSONAL DATA**

- 1.1 With respect to the Parties' rights and obligations under this Agreement, the Parties acknowledge that the Authority is the Controller and that the Supplier is the Processor, and that the processing may not be determined by the Supplier.
- 1.2 The Supplier shall:
- (a) not Process or transfer the Personal Data other than in accordance with the Authority's written instructions, as set out in Schedule A (*Data Processing and List of Sub-processors*), unless required by EU or member state law or UK Law to which the Supplier is subject, in which case the Supplier shall promptly inform the Authority of that legal requirement before Processing or transferring that Personal Data, unless prohibited by law;
  - (b) acknowledge that the provision of the Services is restricted to the Processing of the types of Personal Data and categories of Data Subject set out in Part 1 of Schedule A (*Data Processing and List of Sub-processors*), and shall, with the Authority's written consent, update the details in Schedule A (*Data Processing and List of Sub-processors*) from time to time as necessary;
  - (c) ensure that at all times it has in place appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the Personal Data, Personal Data Breaches and/or accidental loss, destruction or damage to the Personal Data, and having regard to the:
    - (i) nature of the data to be protected;
    - (ii) harm that might result from a Personal Data Breach;
    - (iii) state of technological development; and
    - (iv) cost of implementing any measures;
  - (d) not disclose or transfer the Personal Data to any third party or Supplier Personnel unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, obtain the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Agreement);
  - (e) take all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data] and ensure that the Supplier Personnel:
    - (i) are aware of and comply with the Supplier's duties under this Clause 1;
    - (ii) are subject to confidentiality undertakings or professional or statutory obligations of confidentiality;
    - (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 Authority or as otherwise permitted by this Agreement;
    - (iv) have undergone adequate training in the use, care, protection and

handling of Personal Data (as defined in the Relevant Data Protection Laws); and

- (v) retain evidence of the steps taken in respect of Clauses 23.1(e)(i) to 23.1(e)(iv) above for the Authority's inspection;
- (f) notify the Authority immediately upon becoming aware of a reasonably suspected, "near-miss" or actual Personal Data Breach or circumstances that may give rise to a Personal Data Breach, providing the Authority with sufficient information and in a timescale which allows the Authority to meet its obligations to report a Personal Data Breach within 72 hours under Article 33 of the GDPR. Such notification shall as a minimum:
  - (i) describe the nature of the Personal Data Breach, the categories and approximate numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
  - (ii) communicate the name and contact details of the Data Protection Officer or other relevant contact from whom more information may be obtained;
  - (iii) describe the likely consequences of the Personal Data Breach; and
  - (iv) Describe the measures taken or proposed to be taken to address the Personal Data Breach.
- (g) co-operate with the Authority and take such reasonable commercial steps as are directed by it to mitigate or remedy the consequences of a reasonably suspected, "near-miss" or actual Personal Data Breach including but not limited to:
  - (i) documenting any such Personal Data Breaches and reporting them to any supervisory authority;
  - (ii) taking measures to address any such Personal Data Breaches, including where appropriate, measures to mitigate their possible adverse effects; and
  - (iii) conducting Data Protection Impact Assessments of any Processing operations and consulting any supervisory authorities, Data Subjects and their representatives accordingly;
- (h) notify the Authority immediately if it receives:
  - (i) from a Data Subject (or third party on their behalf):
    - (A) a Data Subject Access Request (or purported Data Subject Access Request);
    - (B) a request to rectify, any inaccurate Personal Data;
    - (C) a request to have any Personal Data erased;
    - (D) a request to restrict the Processing of any Personal Data;
    - (E) a request to obtain a portable copy of part of the Personal Data, or to transfer such a copy to any third party;
    - (F) an objection to any Processing of Personal Data;

- (G) any other request, complaint or communication relating to the Authority's obligations under the Relevant Data Protection Laws;
    - (ii) any communication from the Information Commissioner's Office or any other regulatory authority in connection with Personal Data; or
    - (iii) a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
  - (i) not, without the Authority's prior written consent, make or permit any announcement in respect of a Personal Data Breach or respond to any request, communication or complaint of the kind listed at Clause 1.2(h)(i)-(iii);
  - (j) taking into account the nature of the processing, provide the Authority with full assistance in relation to either Party's obligations under the Relevant Data Protection Laws and any complaint, communication or request as listed at Clause 1.2(h) (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:
    - (i) the Authority with full details and copies of the complaint, communication or request;
    - (ii) such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Relevant Data Protection Laws;
    - (iii) the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;
    - (iv) assistance as requested by the Authority following any Personal Data Breach;
    - (v) assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office.
- 1.3 The Supplier's obligation to notify under Clause 1.2(f) and 1.2(h) shall include the provision of further information to the Authority in phases, as details become available.
- 1.4 Not used
- 1.5 The Supplier must obtain the prior written consent of the Authority before appointing any Sub-contractor or other third party to Process any Personal Data ("**Sub-processor**") and the Supplier shall remain fully liable to the Authority for any failure by a Sub-processor to fulfil its obligations in relation to the Processing of any Personal Data. Such consent shall be conditional upon:
- (a) the use of any Sub-processor being otherwise in accordance with 1.7; and
  - (b) the Supplier entering into a continuing obligation to provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

- 1.6 In accordance with Clause 1.5, the Authority consents to the use by the Supplier as at the Effective Date of the Sub-processors listed in Part B of Schedule A (*Data Processing and List of Sub-processors*) which shall be updated as required with the written consent of the Authority.
- 1.7 The Supplier shall procure that all Sub-processors:
- (a) prior to commencing the Processing of any Personal Data enter into a written contract in relation to the Processing with either the Authority or the Supplier which shall include substantially the same data protection obligations on the Sub-processor as are imposed on the Supplier by these Terms and Conditions and which shall set out the Sub-processor's agreed Processing activities in the same or substantially similar form as provided at Part A of Schedule A to these General Terms and Conditions; or
  - (b) insofar as the contract referred to at paragraph (a) above involves the transfer of Personal Data to any Off-shore Location in accordance with Clause 1.8, it shall incorporate the Standard Contractual Clauses or such other mechanism as directed by the Authority to ensure the adequate protection of the transferred Personal Data;
  - (c) act in accordance with this Clause 1.
- 1.8 The Supplier shall not Process or otherwise transfer any Personal Data in or to any Off-shore Location (unless the transfer is required by EU or member state law to which the Supplier is subject, and if this is the case then the Supplier shall inform the Authority of that legal requirement before Processing that Personal Data, unless that law prohibits such information being provided). If, after the Effective Date, the Supplier or any Sub-contractor wishes to Process and/or transfer any Personal Data [and/or Sanitised Personal Data] in or to any Off-shore Location, the following provisions shall apply:
- (a) the Supplier shall submit a Change Request to the Authority which, if the Authority agrees, at its sole discretion, to such Change Request, shall be dealt with in accordance with the Change Control Procedure and Clauses 1.8(b) to 1.8(d);
  - (b) the Supplier shall set out in its Change Request and/or Impact Assessment details of the following:
    - (i) the Personal Data [and/or Sanitised Personal Data] which will be transferred to and/or Processed in any Off-shore Location;
    - (ii) the Off-shore Location or Countries which the Personal Data [and/or Sanitised Personal Data] will be transferred to and/or Processed in;
    - (iii) any Sub-contractors or other third parties who will be Processing and/or receiving Personal Data [and/or Sanitised Personal Data] in an Off-shore Location; and
    - (iv) how the Supplier will ensure an adequate level of protection and adequate safeguards in respect of the Personal Data that will be Processed in and/or transferred to Off-Shore Location(s) so as to ensure the Authority's compliance with the Relevant Data Protection Laws;
  - (c) in providing and evaluating the Change Request and Impact Assessment, the Parties shall ensure that they have regard to and comply with then-current

Authority, Central Government Bodies and Information Commissioner Office policies, procedures, guidance and codes of practice on, and any approvals processes in connection with, the Processing in and/or transfers of Personal Data [and/or Sanitised Personal Data] to any Off-shore Location; and

- (d) the Supplier shall comply with such other instructions and shall carry out such other actions as the Authority may notify in writing, including:
- (i) incorporating Relevant Data Protection Laws Standard Contractual Clauses into this Agreement or a separate data processing agreement between the Parties; and
  - (ii) complying with the provisions of Clauses 1.5 – 1.7 in relation to any Sub-contractor or other third party who will be Processing and/or receiving or accessing the Personal Data [and/or Sanitised Personal Data] in any Off-shore Location either enters into:
    - (A) a direct data processing agreement with the Authority on such terms as may be required by the Authority; or
    - (B) a data processing agreement with the Supplier on terms which are equivalent to those agreed between the Authority and the Sub-contractor relating to the relevant Personal Data [and/or Sanitised Personal Data] transfer,

and in each case which the Supplier acknowledges may include the incorporation of Relevant Data Protection Laws Standard Contractual Clauses and technical and organisation measures which the Authority deems necessary for the purpose of protecting Personal Data [and/or Sanitised Personal Data].]

1.9 The Supplier shall ensure that the Authority complies with any obligations under the Relevant Data Protection Laws and shall not perform its obligations under this Agreement in such a way as to cause the Authority to breach any of the Authority's obligations under the Relevant Data Protection Laws to the extent the Supplier is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations. In connection with this obligation, the Supplier shall:

- (a) immediately inform the Authority if, in its opinion, any instruction infringes, or might reasonably be considered to infringe, the Relevant Data Protection Laws;
- (b) provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any processing, such assistance including, at the discretion of the Authority:
  - (i) a systematic description of the envisaged processing operations and the purpose of the processing;
  - (ii) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
  - (iii) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal

Data;

- (c) implement, review and maintain organisational and technical security measures to ensure the security of Personal Data in accordance with Article 32 of the GDPR, including by:
  - (i) pseudonymising or encrypting Personal Data with the written consent of the Authority;
  - (ii) ensuring the on-going confidentiality, integrity, availability and resilience of Processing systems and services;
  - (iii) ensuring a means to restore the availability of and access to Personal Data in a timely manner following any physical or technical incident; and
  - (iv) having in place a process for regularly testing, assessing and evaluating the effectiveness of the organisational and technical security measures; and
- (d) at the written direction of the Authority, promptly and securely delete or return to the Authority or transfer to any Replacement Supplier Personal Data (and any copies of it) in such format as is requested by the Authority, unless the Supplier is required by Law to retain the Personal Data.

1.10 The Supplier shall not cause the Authority to breach any obligation under the Relevant Data Protection Laws and shall itself comply fully with its obligations under the Relevant Data Protection Laws including by:

- (a) adhering to any relevant codes of conduct published pursuant to Article 40 of the GDPR;
- (b) designating a Data Protection Officer if required by the Relevant Data Protection Laws;
- (c) maintaining complete and accurate records of its Processing of Personal Data containing the information set out in Article 30(2) of the GDPR, this requirement applying only where the Supplier employs 250 or more staff, unless:
  - (i) the Processing is not occasional;
  - (ii) 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 Processing is likely to result in a risk to the rights and freedoms of Data Subjects; and
- (d) reporting any suspected non-compliance or actual non-compliance with this Clause to the Authority immediately upon becoming aware of such non-compliance.

1.11 The Supplier shall allow for audits of its Data Processing activity by the Authority or the Authority's designated auditor, and make available to the Authority or the Authority's

designated auditor all information necessary to demonstrate compliance with this Clause.

- 1.12 For the avoidance of doubt, nothing in these Terms and Conditions relieves the Supplier of its own direct responsibilities and liabilities under the GDPR.

## **DEFINITIONS**

<b>“Controller”</b>	has the meaning given in the Relevant Data Protection Laws;
<b>“Data Protection Impact Assessment”</b>	means an assessment by the Controller of the impact of the processing on the protection of Personal Data;
<b>“Data Protection Officer”</b>	has the meaning given in the Relevant Data Protection Laws;
<b>“Data Subject”</b>	has the meaning given in the Relevant Data Protection Laws;
<b>“Data Subject Access Request”</b>	a request made by a Data Subject in accordance with rights granted pursuant to the Relevant Data Protection Laws to access his or her Personal Data;
<b>"GDPR"</b>	means the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data being enforced in the EU from 25 May 2018 (repealing Directive 95/46/EC), along with the codes of practice, codes of conduct, regulatory guidance and standard clauses and other related or equivalent domestic legislation, as updated from time to time;
<b>“Personal Data”</b>	personal data (as defined in the Relevant Data Protection Laws) which is Processed by the Supplier or any Sub-contractor pursuant to or in connection with this Agreement;
<b>“Personal Data Breach”</b>	means: <ul style="list-style-type: none"><li>(a) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed;</li><li>(b) a discovery or reasonable suspicion that there is a vulnerability in any technological measure used to protect any Personal Data that has previously been subject to a breach within the scope of</li></ul>

paragraph (a), which may result in exploitation or exposure of that Personal Data; or

- (c) any defect or vulnerability with the potential to impact the ongoing resilience, security and/or integrity of systems Processing Personal Data;

**“Process”** has the meaning given to it under the Relevant Data Protection Laws and **“Processed”** and **“Processing”** shall be construed accordingly;

**“Processor”** has the meaning given in the Relevant Data Protection Laws;

**“Relevant Data Protection Laws”** means: (i) the Data Protection Act 1998 and, at such time as it is superseded, the Data Protection Act 2018 [subject to being given Royal Assent]; (ii) the GDPR, the Law Enforcement Directive (Directive EU 2016/680) and any applicable national implementing Laws as amended from time to time; (iii) any other applicable Laws relating to the processing of personal data and privacy; and (iv) all applicable guidance, standard terms, codes of practice and codes of conduct issued by the Information Commissioner and other relevant regulatory, supervisory and legislative bodies in relation to such Laws;

**"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission or a supervisory authority (as such term is defined by the GDPR) which subsequently amends, replaces or supersedes these.

## **7.2 Contract Management Plan and Management Information**

### **1 MANAGEMENT OF THE SERVICES**

- 1.1 Both Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Agreement can be fully realised.
- 1.2 Both Parties shall pro-actively manage risks attributed to them under the terms of this Agreement and the Supplier shall develop, operate, maintain and (as appropriate) amend processes for the identification and management of risks and issues.
- 1.3 The Supplier shall provide to the Authority's representatives access to all relevant documentation and/or any part of the Supplier's (or its sub-contractor's) premises as may be reasonably requested by the Authority's representatives, including for the purpose of commercial assurance, risk assessment, security assurance, familiarisation on procedures, audit of the Supplier's compliance with this Agreement and/or site audits. Full details of the Authority's requirement and timescales for the provision of management information reports are set out in Paragraph 3.
- 1.4 The Authority reserves the right to attend meetings between the Supplier and any subcontractors it utilises to provide the service to ensure proper oversight, management, delivery and performance of the Services and the Supplier shall procure that the Authority has access to such meetings.

### **2 EFFICIENCY SAVINGS**

- 2.1 As part of routine contract management activities the Supplier will be required to work with the Authority to realise any possible efficiency savings during the Term. Possible efficiency savings will be reviewed during review meetings pursuant to Paragraph 3 and any savings realised annually will be distributed between the Supplier and the Authority as agreed in advance.

### **3 REVIEWS**

- 3.1 The Parties shall attend annual performance review meetings, on a date to be agreed between the Parties or, in the absence of such agreement, within 30 Working Days of each anniversary of the Effective Date, to consider the progress of the Agreement, discuss the management information reports and to review any operational issues that have arisen in the preceding review meetings on the following basis.
- 3.2 The Parties shall agree the format of the review meetings (for example, face to face or telephone conference) in advance.
- 3.3 The Supplier must provide the Authority with the most up to date management information relating to the period under review at least 5 Working Days before any review meeting.
- 3.4 Each Party shall procure that those of its contract management team representatives whose attendance is reasonably required to achieve the aims and objectives of the meeting, and any other persons considered by the Authority to be necessary for the review, make all reasonable efforts to attend review meetings.
- 3.5 In respect of the period under review, the Authority will take into account any matters it considers necessary, including:
  - 3.5.1 the Supplier's performance in respect of the service levels and KPI's as detailed at Schedule 2 (including any relevant service level trends analysis and whether the service levels reflect improvements in the Services over the Term and any efficiency gains made by the Supplier);

3.5.2 consideration of any changes which may need to be made to the Services; and

3.5.3 a review of future requirements in relation to the Services.

- 3.6 The Authority shall prepare a report containing its findings from the annual review and discuss with the Supplier how any proposed changes to the Agreement and/or to the Services shall be addressed. Any Contract Changes to be implemented in accordance with this Paragraph shall be implemented in accordance with Schedule 4 (Change Control Procedure).

#### 4 CONTRACT MANAGEMENT ROLES AND DISPUTE ESCALATION POINTS

- 4.1 The Parties shall assign personnel with the appropriate skills and experience to perform the roles and responsibilities listed in the table below.

Role	Key Personnel	Responsibilities	Contact Name, Title & Contact Details	
			Authority	Supplier
	No	Overall responsibility for delivery of the Agreement. Level 3 escalation point	<b>J Holliday</b>	
	No	Overall responsibility for the commercial integrity of the Agreement. Level 2 escalation point	<b>A Bexfield</b>	
	No	Responsible for overseeing the contract review process. Level 1 escalation point	<b>M Barrett</b>	
Commercial Manager	Yes	Responsible for managing the change control process.	<b>A Cullenaine</b>	
Contract Manager	Yes	Responsible for the day to day	<b>A Bexfield</b>	

		management of the Agreement.		
--	--	------------------------------	--	--

- 4.2 In the event that the Supplier wishes to replace any of its representatives in the roles listed in Paragraph 4.1, the Supplier shall notify the Authority in writing of the proposed change for the Authority's agreement (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing it is intended that each Authority representative has at all times a counterpart representative of equivalent seniority and expertise.
- 4.3 The Authority may, by written notice to the Supplier, revoke or amend the authority of any of its representatives in the roles listed in Paragraph 4.1 or appoint a new representative into the role.

## 5 ADDRESS FOR NOTICES

- 5.1 The address for notices of the Parties are:

### Authority

HM Revenue and Customs  
100 Parliament Street, Westminster,  
London, SW1A 2BQ

Attention: Adam Garside

Email: [Adam.Garside@hmrc.gsi.gov.uk](mailto:Adam.Garside@hmrc.gsi.gov.uk)

### Supplier

KPMG, 15 Canada Square,  
Canary Wharf,  
London

Attention: Andrew North

Email: [\[mailto:andrew.c.north@kpmg.co.uk\]](mailto:andrew.c.north@kpmg.co.uk)

## 7.3 Change Control Procedure

### 1 CHANGE CONTROL PROCEDURE

- 1.1 Either Party may propose a change to this Agreement ("**Contract Change**") in accordance with the procedure for changing the Agreement set out in this Schedule ("**Change Control Procedure**").
- 1.2 If either Party wishes to propose a Contract Change it shall submit to the other Party a written request substantially in the form set out in Annex 1 detailing the proposed Contract Change ("**Change Request**") specifying, in as much detail as is reasonably practicable, the nature of the proposed Contract Change. As soon as reasonably practicable but in any event within ten (10) Working Days of receipt or issue of a Change Request (as the case may be) the Supplier shall submit to the Authority a written assessment of the Change Request ("**Impact Assessment**").
- 1.3 Each Impact Assessment shall be completed in good faith and shall include the following information (except where such information is not relevant to the proposed Contract Change):
- 1.3.1 details of the proposed Contract Change including the reason for the Contract Change;
  - 1.3.2 details of the impact of the proposed Contract Change on the Services and the Supplier's ability to meet its other obligations under this Agreement;
  - 1.3.3 any variations to the terms of this Agreement that will be required as a result of that impact, including proposed changes to the service levels or KPIs or any timetable

- previously agreed by the Parties;
  - 1.3.4 details of the cost of implementing the proposed Contract Change;
  - 1.3.5 details of the ongoing costs required by the proposed Contract Change when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;
  - 1.3.6 a timetable and high level plan for the mobilisation of the proposed Contract Change;
  - 1.3.7 details of how the proposed Contract Change will ensure compliance with any applicable Change in Law;
  - 1.3.8 an assessment of the possible risks of introducing the proposed Contract Change; and
  - 1.3.9 such other information as the Authority may reasonably request in (or in response to) the Change Request
- 1.4 Within fifteen (15) Working Days of receipt of the Impact Assessment, the Authority shall evaluate the Change Request and Impact Assessment and shall notify the Supplier whether it approves or rejects the proposed Contract Change or whether it requires the Supplier to make any changes to the Impact Assessment. If the Authority requires the Supplier to make such changes, the Supplier shall make such modifications within five (5) Working Days of request.
- 1.5 If the Authority notifies the Supplier that it accepts the proposed Contract Change, then the Supplier shall prepare two (2) copies of a change authorisation note substantially in the form set out in Annex 2 (“**Change Authorisation Note**”) which it shall sign and deliver to the Authority for its signature. Following receipt by the Authority of the Change Authorisation Note, it shall sign both copies and return one copy to the Supplier.
- 1.6 Until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 1.5, then:
- 1.6.1 unless the Authority expressly agrees (or requires) otherwise in writing, the Supplier shall continue to supply the Services in accordance with the existing terms of this Agreement as if the proposed Contract Change did not apply; and
  - 1.6.2 any discussions, negotiations or other communications which may take place between the Authority and the Supplier in connection with any proposed Contract Change shall be without prejudice to each Party’s other rights under this Agreement.

## **2 SUPPLIER’S RIGHT OF REJECTION**

- 2.1 The Supplier shall have the right to reject a Change Request solely in the manner set out in Paragraph 2.2.
- 2.2 Following an Impact Assessment, if:
- 2.2.1 the Supplier reasonably believes that any proposed Contract Change which is requested by the Authority would:
    - (a) materially and adversely affect the risks to the health and safety of any person; and/or
    - (b) require the Services to be performed in a way that infringes any Law; and/or
  - 2.2.2 the Supplier demonstrates to the Authority's reasonable satisfaction that the proposed Contract Change is technically impossible to implement and neither the Supplier Solution nor the Services Description state that the Supplier does have the technical capacity and flexibility required to implement the proposed Contract

Change,

then the Supplier shall be entitled to reject the proposed Contract Change and shall notify the Authority of its reasons for doing so within five (5) Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to Paragraph 1.2.

### 3 FAST TRACK CHANGES

3.1 The parties acknowledge to ensure operational efficiency that there may be circumstances where it is desirable to expedite the processes set out above.

3.2 If :

3.2.1 the total number of Contract Changes in relation to which the expedited procedure in this Paragraph 3 ("**Fast-track Change Procedure**") has been applied does not exceed four (4) in any twelve (12) month period; and

3.2.2 both Parties agree the value of the proposed Contract Change over the remaining Term does not exceed £5,000 and the proposed Contract Change is not significant (as determined by the Authority acting reasonably),

then the parties shall confirm to each other in writing that they shall use the process set out in paragraphs 1 and 2 above but with reduced timescales, such that any period of fifteen (15) Working Days is reduced to five (5) Working Days, any period of ten (10) Working Days is reduced to two (2) Working Days and any period of five (5) Working Days is reduced to one (1) Working Day.

3.3 The Parties may agree in writing to revise the parameters set out in Paragraph 3.2 from time to time or that the Fast-track Change Procedure shall be used in relation to a particular Contract Change notwithstanding that the total number of Contract Changes to which such procedure is applied will then exceed four (4) in a twelve (12) month period.

### 4 OPERATIONAL CHANGE PROCEDURE

4.1 Any change in the Supplier's operational procedures which the Parties agree in all respects, when implemented:

4.1.1 will not affect the Charges and will not result in any other costs to the Authority;

4.1.2 may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services;

4.1.3 will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure; and

4.1.4 will not require a change to this Agreement,

(an "**Operational Change**") shall be processed in accordance with this Paragraph 4.

4.2 Any Operational Changes identified by the Supplier to improve operational efficiency of the Services may be implemented by the Supplier without following the Change Control Procedure for proposed Contract Changes provided they do not:

4.2.1 have an impact on the business of the Authority;

4.2.2 require a change to this Agreement;

4.2.3 have a direct impact on use of the Services; or

4.2.4 involve the Authority in paying any additional Charges or other costs.

4.3 The Authority may request an Operational Change by submitting a written request for Operational Change ("**RFOC**") to the Supplier's contract manager (whose details are set out in Paragraph 4 of Schedule 3).

- 4.4 The RFOC shall include the following details:
  - 4.4.1 the proposed Operational Change; and
  - 4.4.2 the timescale for completion of the Operational Change.
- 4.5 The Supplier shall inform the Authority of any impact on the Services that may arise from the proposed Operational Change.
- 4.6 The Supplier shall complete the Operational Change by the timescale specified for completion of the Operational Change in the RFOC, and shall promptly notify the Authority when the Operational Change is completed.

## **5 IMPLEMENTATION OF CONTRACT CHANGES**

- 5.1 The Parties shall meet as required and on request by either Party to discuss the order in which agreed Contract Changes are implemented and to monitor the implementation of such Contract Changes.

## **6 CHARGES FOR CONTRACT CHANGES**

- 6.1 Each Party will be responsible for any costs they incur as a result of preparing a Change Request or Impact Assessment.
- 6.2 Both Parties must take all reasonable steps to avoid or minimise additional Charges arising from the implementation of any Contract Change, including where possible using resources already deployed in providing the Services at no additional cost. If additional resources or costs will be required then the Parties must calculate the cost of the Contract Change in accordance with Schedule 1, Paragraph A5.

## **7 INDEXATION**

- 7.1 For the avoidance of doubt, the Supplier may not vary Charges to take account of Indexation at any time.

**ANNEX 1: CHANGE REQUEST FORM**

CR NO.:	TITLE:	TYPE OF CHANGE (e.g. FAST TRACK):
CONTRACT:		REQUIRED BY DATE:
ACTION:	NAME:	DATE:
RAISED BY:		
AREA(S) IMPACTED ( <i>OPTIONAL FIELD</i> ):		
ASSIGNED FOR IMPACT ASSESSMENT BY:		
ASSIGNED FOR IMPACT ASSESSMENT TO:		
SUPPLIER REFERENCE NO.:		
FULL DESCRIPTION OF REQUESTED CONTRACT CHANGE (INCLUDING PROPOSED CHANGES TO THE WORDING OF THE AGREEMENT):		
DETAILS OF ANY PROPOSED ALTERNATIVE SCENARIOS:		
REASONS FOR AND BENEFITS AND DISADVANTAGES OF REQUESTED CONTRACT CHANGE:		
SIGNATURE OF REQUESTING CHANGE OWNER:		
DATE OF REQUEST:		

**ANNEX 2: CHANGE AUTHORISATION NOTE**

CR NO.:	TITLE:	DATE RAISED:
CONTRACT:	TYPE OF CHANGE:	REQUIRED BY DATE:
REASON FOR THE CHANGE:		
DETAILED DESCRIPTION OF CONTRACT CHANGE (GIVING FULL DETAILS, INCLUDING ANY SPECIFICATIONS); AND WORDING OF RELATED CHANGES TO THE AGREEMENT:		
COST OF THE CHANGE:		
TIMETABLE:		
IMPACT ON THE AGREEMENT:		
SIGNED ON BEHALF OF THE AUTHORITY:		SIGNED ON BEHALF OF THE SUPPLIER:
Signature:_____		Signature:_____
Name:_____		Name:_____
Position:_____		Position:_____
Date:_____		Date:_____

**7.2 Amendments to/refinements of the Call Off Terms**

Not Used

**7.3 Alternative and/or Additional Clauses (select from Call Off Schedule 14 (Alternative and/or Additional Clauses))**

Not used

**8. FORMATION OF CALL OFF CONTRACT**

**8.1 BY SIGNING AND RETURNING THIS ORDER FORM (which may be done by electronic means) the Supplier agrees to enter a Call Off Contract with the Customer to provide the Services.**

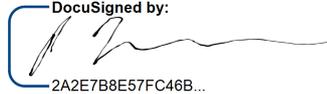
**8.2 The Parties hereby acknowledge and agree that they have read the Order Form and the Call Off Terms and by signing below agree to be bound by this Call Off Contract.**

**8.3 In accordance with paragraph 7 of Framework Schedule 5 (Call Off Procedure), the Parties hereby acknowledge and agree that this Call Off Contract shall be formed when the Customer acknowledges (which may be done by electronic means) the receipt of the signed copy of the Order Form from the Supplier within two (2) Working Days from receipt.**

**For and on behalf of the Supplier:**

Name and Title	Andrew North Director
Signature	 <p>DocuSigned by: Andrew North D766BBD04BE54CA...</p>
Date	2/8/2019

**For and on behalf of the Customer:**

Name and Title	Pete Gleeson Assistant Director Sourcing
Signature	 <p>DocuSigned by: Pete Gleeson 2A2E7B8E57FC46B...</p>
Date	2/8/2019