

Crown Commercial Service

Call Off Order Form for Public Sector Resourcing Model Services

PUBLIC SECTOR RESOURCING CALL OFF ORDER FORM AND PUBLIC SECTOR RESOURCING CALL OFF TERMS

PART 1 – PUBLIC SECTOR RESOURCING CALL OFF ORDER FORM

SECTION A

This Call Off Order Form is issued in accordance with the provisions of the Framework Agreement for the provision of **Public Sector Resourcing Model Services** dated 16/01/2018 (“**Framework Agreement**”).

The Service Provider agrees to supply the Services specified below on and subject to the terms of this Call Off Contract.

For the avoidance of doubt this Call Off Contract consists of the terms set out in this Call Off Order Form and the Call Off Terms. The words and expressions in this Call Off Order Form shall have the meanings given to them in the Call Off Terms and the Framework Agreement).

This Call Off Order Form shall comprise the following [delete as applicable]:

- this document headed “Call Off Order Form for Public Sector Resourcing Model Services (“Call Off Order Form”)
- Appendix 1 – Not Used
- Appendix 2 – Call-Off Schedule 20 (Authorised Processing Template)
- Appendix 3 – Performance Reporting and Monitoring (Governance Pack)
- Appendix 4 – Schedule of Additional Services
- Appendix 5 – Security Management Plan
- Appendix 6 – Transition Workers

From	UK HEALTH SECURITY AGENCY whose registered office is at Nobel House, 17 Smith Square, London, SW1P 3HX (" CUSTOMER ") [REDACTED] (" CUSTOMER REPRESENTATIVE ")
To	ALEXANDER MANN SOLUTIONS LIMITED (Company Registration Number 02073305) whose registered office is at 7-10 Bishopsgate, London EC2N 3AQ (" SERVICE PROVIDER ") [REDACTED] (" SERVICE PROVIDER REPRESENTATIVE ")

SECTION B

CALL OFF CONTRACT PERIOD

1.1.	<p>TERM:</p> <p>The term of this Call Off Contract shall be from and including 1st April 2022 (the "Service Commencement Date") until 17th January 2024 ("Initial Call Off Period").</p> <p>The Customer shall have the option to extend the Call Off Contract Period for a further term following expiry of the Initial Call Off Period ("Call Off Extension Period"), such Call Off Extension Period to expire no later than:</p> <ul style="list-style-type: none">(i) 18 months after the expiry of the Framework Agreement; or(ii) where the Framework Agreement has been terminated earlier in accordance with the Framework Agreement, 18 months after the Framework Agreement has been deemed to terminate, whichever is the earlier. <p>The Customer's extension of this Call Off Contract for the Call Off Extension Period shall be subject to:</p> <ul style="list-style-type: none">(a) the Customer obtaining all relevant approvals required to operate such extension; and(b) the Customer providing no less than 20 Working Days' written notice prior to expiry of the Initial Call Off Period to the Service Provider that the Customer wishes to exercise its right to extend the Call Off Contract and stating the duration of the Call Off Extension Period.
-------------	---

SERVICES

2.1	<p>SERVICES REQUIRED: As specified in Call Off Terms Schedule 2 (Services)</p>
2.2	<p>ON BOARDING AND SECURITY VETTING</p> <p>Unless otherwise specified in this paragraph 2.2 the provisions of Clause 9.3.1 (Schedule 2: Services) shall apply.</p> <p>For the avoidance of doubt, in the event that a Customer requests any additional vetting, security checks or an NHS Work Health Assessment for any Worker or category of Workers, it may be at the Customer's cost. Such costs shall be agreed prior to the commencement of the Services and may include a reasonable charge to reflect the administrative burden on AMS.</p>

IMPLEMENTATION PLAN

3.1	<p>IMPLEMENTATION PLAN: If an Implementation Plan is required by the Customer, a tailored plan should be agreed by the Parties and attached to this paragraph, as Appendix 1: Implementation Plan.</p>
3.2	<p>In signing this Call Off Order Form the Service Provider confirms that prior to the Service Commencement Date the Customer has been successfully onboarded onto the Service Provider's Vendor Management System under the terms of the Department of Health and Social Care Call Off Contract, such that there is no requirement for an Implementation Plan to be agreed.</p>

CONTRACT PERFORMANCE

4.1	STANDARDS: As referenced in Clause 11 and Schedule 1 (Definitions) of the Call Off Contract.
4.2	KPI'S: As referenced in Schedule 18 of the Call Off Contract, as amended by agreement between the Authority and the Service Provider. The process for monitoring and reporting on performance against the KPIs is set out in Appendix 3 (Customer Governance Performance Reporting and Monitoring)
4.3	PERIOD FOR PROVIDING RECTIFICATION PLAN: As per Clause 38.2.1(a) of the Call Off Terms.

PAYMENT

5.1	CALL OFF CONTRACT CHARGES (including any applicable discount(s), but excluding VAT): Subject to this paragraph 5.1 as per Annex 1 of Schedule 3 (Call Off Contract Charges, Payment and Invoicing) of the Call Off Terms, Contract Charges may be amended to reflect increase/decrease in market rates as the result of benchmarking of the Services throughout the life of this Call Off Contract.
5.2	PAYMENT TERMS/PROFILE (including method of payment e.g. Government Procurement Card (GPC) or BACS): As per Annex 2 of Call Off Terms Schedule 3 (Call Off Contract Charges, Payment and Invoicing). On average payment to be made in line with the Procurement Policy Note 05/15 as per the following link; https://www.gov.uk/government/publications/procurement-policy-note-0515-prompt-payment-and-performance-reporting The Service Provider will invoice the Customer each week following the draw down of approved timesheets from the VMS or other appropriate collation of approved manual timesheets as the case may be in accordance with Call Off Terms Schedule 3 (Call Off Contract Charges, Payment and Invoicing, Clause 7.
5.3	Reimbursable Expenses Pre-approved expenses incurred by Workers only.
5.4	CUSTOMER BILLING ADDRESS (paragraph 7.6 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing). UKHSA Accounts Payable Team UK Health Security Agency Manor Farm Road Porton Down Salisbury SP4 0JG

LIABILITY AND INSURANCE


6.1	ESTIMATED YEAR 1 CALL OFF CONTRACT CHARGES:
------------	--

	<p>The sum of £ 1,800,000</p> <p>The Year 1 Call-off Contract Charges should be calculated on the basis of the estimated charges to the Service Provider only. This would be calculated by using the 'Managed Service Provider' Fees and the 'Route To Talent' Fees only as shown in Annex 1 of Call-off Schedule 3 (Call-off Contract Charges, Payment and Invoicing).</p>
6.2	SERVICE PROVIDER'S LIMITATION OF LIABILITY As per Clause 36.2.1 of the Call Off Terms.

TERMINATION AND EXIT

7.1	TERMINATION ON MATERIAL DEFAULT As per Clause 41.2.1(c) of the Call Off Terms.
7.2	TERMINATION WITHOUT CAUSE NOTICE PERIOD As per Clause 41.7.1 of the Call Off Terms.
7.3	UNDISPUTED SUMS LIMIT: for the purposes of Clause 42.1.1 of the Call Off Terms the Undisputed Sums Limit shall be three months' average Call Off Contract Charges.
7.4	<p>EXIT MANAGEMENT</p> <p>Notwithstanding Call Off Schedule 9 (Exit Management), an initial Exit Plan ("Exit Plan") has been agreed with the Authority and is available from the Authority, on demand. The Exit Plan will be developed further by the Service Provider and the Authority within 6 months of a planned exit.</p>

OTHER CALL OFF REQUIREMENTS

8.1	SECURITY:	<i>The PSR Security Management Plan has been updated by agreement between the parties and is attached in Appendix 5 hereto</i>
8.2	<p>ICT POLICY:</p> <p>The following documents constitute the Customer's ICT Policy:</p>  <p>UKHSA ICT Policy.zip</p>	
8.3	NOT USED	
8.4	PROTECTION OF CUSTOMER DATA:	As per Clause 34.2 of the Call Off Terms.
8.5	<p>NOTICES (Clause 55.6 of the Call Off Terms):</p> <p>Customer's postal address and email address:</p> <p style="padding-left: 40px;">UK Health Security Agency Nobel House, 17 Smith Square, London, SW1P 3HX professionalservicescontractmanagementteam@dhsc.gov.uk</p> <p>Service Provider's postal address and email address:</p>	

7-11 Bishopsgate, London, EC2N 3AQ



8.6

NEW DEFINITIONS

The definitions set out in the Call Off Terms (Schedule 1: Definitions) shall be varied as follows (additions and/or deletions are identified as underlined, italicised and/or strike-through):

"Contracting Authorities Authorised Users"	means any of the Contracting Authorities' personnel who access the Services;
"Customer Data"	means: <ul style="list-style-type: none">a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any Customer's Confidential Information, and which:<ul style="list-style-type: none">i) are supplied to the Service Provider by or on behalf of the Customer; orii) the Service Provider is required to generate, process, store or transmit pursuant to this Call Off Contract; or any Personal Data for which the Customer is the Data Controller;
"Data Controller"	has the meaning given to it in the Data Protection Act 1998, as amended from time to time;
"Data Processor"	has the meaning given to it in the Data Protection Act 1998, as amended from time to time;
<u>"Independent Control"</u>	<i><u>where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "Independent Controller" shall be construed accordingly;</u></i>
<u>"Information Commissioner"</u>	<i><u>the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;</u></i>

	<u>"Inside IR35"</u>	<u>means the circumstances under which the Worker will provide the Services under the Assignment are such that Section 61N ITEPA applies (i.e. worker is treated as receiving earnings from employment);</u>
	<u>"ITEPA"</u>	<u>means the Income Tax (Earnings and Pensions) Act 2003</u>
	<u>"Joint Controllers"</u>	<u>where two or more Controllers jointly determine the purposes and means of Processing;</u>
	<u>"Off-Payroll IR35 Legislation"</u>	<u>means ITEPA Part 2, Chapter 10;</u>
	<u>"Outside IR35"</u>	<u>means the circumstances under which the Worker will provide the Services are such that Section 61N ITEPA does not apply (i.e. worker is not treated as receiving earnings from employment);</u>
	<u>"Processing"</u>	<u>has the meaning given to it in the GDPR and "Process" and "Processed" shall be interpreted accordingly.</u>
	<u>"PSC"</u>	<u>means any "intermediary" (as defined in section 61M ITEPA) in respect of which any of Conditions A – C within section 61N ITEPA are met;</u>
	<u>"Status Determination Statement"</u>	<u>means the written conclusion of the Customer's assessment of the Worker undertaken pursuant to the Off-Payroll IR35 Legislation;</u>
8.7	Transparency Plans See Annex 1 of Call Off Schedule 13 (Transparency Reports)	
8.8	Security Plan; Business Continuity and Disaster Recovery Plan; Equality, Diversity, Economic and Social Value Plan: Notwithstanding Call Off Schedules 7 (Security) the following plans have been agreed with the Authority and are available from the Authority, on demand: <ul style="list-style-type: none"> • Security Plan • Business Continuity and Disaster Recovery Plan • Equality, Diversity, <u>Economic</u> and Social Value Plan Disaster Period: For the purpose of the definition of "Disaster" in Call Off Schedule 1 (Definitions) of the Call Off Terms, the "Disaster Period" shall be one calendar month.	
8.9	ADDITIONAL SERVICES	

	<p>The Service Provider shall provide the additional Customer Services and the Customer shall pay the additional Customer Charges on the terms set out in Appendix 4 hereto.</p>
<p>8.10</p>	<p>OFF-PAYROLL IR35 LEGISLATION</p> <p>The following clauses shall be added to Clause 23 of the Call Off Terms (CALL OFF CONTRACT CHARGES AND PAYMENT):</p> <p>“23.5.3 Subject to clause 23.5.4 the Customer and the Service Provider agree, and the Service Provider warrants and undertakes to the Customer, that no Worker supplied by the Service Provider to the Customer in response to a Requisition will be engaged (directly or indirectly) through a PSC of that Worker.</p> <p>23.5.4 Clause 23.5.3 shall not apply in relation to any Worker under any Assignment existing prior to the Service Commencement Date (“Existing PSC Assignments”) or to any subsequent extensions of any Existing PSC Assignments with such Worker after the Service Commencement Date PROVIDED THAT the Service Provider has specifically notified the Customer in writing, prior to the Service Commencement Date, that such Worker is engaged (directly or indirectly) through a PSC of that Worker.</p> <p>23.5.5 In respect of any Worker falling within clause 23.5.4 (only), the provisions of clauses 23.5.6 – 23.5.9 shall apply and, for the avoidance of doubt, clauses 23.5.6 – 23.5.9 shall not apply, and the Customer shall have no obligation or liability whatsoever under clauses 23.5.6 – 23.5.9, in respect of any Worker and/or any Assignment undertaken by any Worker which does not fall within clause 23.5.4.</p> <p>23.5.6 The Customer acknowledges that it is solely responsible for determining if any Assignment falls Inside IR35 or Outside IR35 pursuant to the Off-Payroll IR35 Legislation and shall be responsible for promptly providing the Service Provider and the Worker with an up-to-date Status Determination Statement for any Worker engaged via a PSC (irrespective of whether the Customer determines that they are Inside or Outside IR35). The Customer will provide such information as the Service Provider may reasonably require in a timely manner to enable the Service Provider to comply with its obligations under the Off-Payroll IR35 Legislation.</p> <p>23.5.7 The Customer will notify the Service Provider immediately if it has reason to believe that the Assignment falls Inside IR35 and/or the nature of the Services or the Assignment and/or its IR35 status has changed or will change.</p> <p>23.5.8 If the Service Provider is notified by either a Subcontractor or a PSC that the Status Determination Statement provided by the Customer is inaccurate, the Service Provider shall notify the Customer as soon as reasonably practicable.</p> <p>23.5.9 The Customer shall be liable for, and shall indemnify the Service Provider against, all Losses incurred, suffered or paid by the Service Provider (including reasonable legal expenses) arising out of or in connection with any of the following:</p>

- a) any incorrect Status Determination Statement by the Customer; and/or
- b) any failure by the Customer to supply to the Worker and the Service Provider, an up-to-date Status Determination Statement in respect of that Worker;
- c) any treatment by the Customer of a Worker who has been categorised under this Agreement following a Status Determination Statement by the Customer as Outside IR35, which treatment causes or contributes to HMRC treating the Worker as being Inside IR35.

23.5.10 The Service Provider shall be liable for, and shall indemnify the Customer against, all Losses incurred, suffered or paid by the Customer (including reasonable legal expenses) arising out of or in connection with:

- a) the failure by the Service Provider, or any other party within the contractual chain between the Service Provider and the relevant PSC, to deduct any tax, national insurance or other statutory deductions, or make any required employer contributions for national insurance or the apprentice levy, where the Service Provider had been given an Inside IR35 Status Determination Statement by the Customer which confirmed that such sums should have been deducted/paid; and/or
- b) the Service Provider breaching the warranty and/or undertaking given by it under clause 23.5.3.

23.5.11 The liability of the Parties under the Call Off Contract with respect to the Off-Payroll IR35 legislation shall be as set out at Clauses 23.5.3 to 23.5.13.

23.5.12 The Parties agree that it shall not be necessary for the Service Provider to comply with the Dispute Resolution Procedure or to notify the Customer in respect of any acts or omissions of the Customer in connection with the Customer's treatment of Workers which may cause an IR35 liability, or subject to Clause 23.5.8, any IR35 status determinations made by the Customer (or decided by the Customer to be unnecessary) in respect of Workers.

23.5.13 It is agreed that the indemnity provided by the Service Provider in clause 23.5.1(b) of the Call Off Terms shall not apply in respect of any Worker under any Assignment falling within clause 23.5.4, and in respect of which the Service Provider has notified the Customer as described in clause 23.5.4, where one of the following scenarios apply:

- a) the Customer does not make a Status Determination Statement in respect of that Worker;
- b) the Customer does not provide the Worker and the Service Provider with a Status Determination Statement in respect of that Worker;
- c) the Customer does not take reasonable care in making a Status Determination Statement in respect of that Worker."

8.11**Independent Controllers**

With effect from 1st January 2021:

8.11.1 The following wording shall be inserted and replace existing clause 34.5.1 of the Call Off Terms:

Status of the Controller

34.5.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Call Off Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) "Controller" in respect of the other Party who is "Processor";
- (b) "Processor" in respect of the other Party who is "Controller";
- (c) "Joint Controller" with the other Party;
- (d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under the Call Off Contract and shall specify in Schedule 20 (Authorised Processing Template) which scenario they think shall apply in each situation

8.11.2 The following clause shall be inserted as a new Clause 34.5.14 of the Call Off Terms:

34.5.14 In the event that the Parties are Joint Controllers in respect of Personal Data under the Call Off Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to Schedule 20.

8.11.3 The following wording shall be inserted as a new Clause 34.6 of the Call Off Terms:

34.6. **"Independent Controllers of Personal Data"**

34.6.1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but in respect of which the Parties are not Joint Controllers, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

34.6.2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

34.6.3. Where a Party has provided Personal Data to the other Party in accordance with Clause 34.5.6 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

- 34.6.4. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Call Off Contract.
- 34.6.5. The Parties shall only provide Personal Data to each other:
- (a) to the extent necessary to perform their respective obligations under the Call Off Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and
 - (c) where it has recorded it in Annex 1 to Call Off Schedule 20 (Authorised Processing Template).
- 34.6.6. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.
- 34.6.7. A Party Processing Personal Data for the purposes of the Framework Agreement shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.
- 34.6.8. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Framework Agreement ("**Request Recipient**"):
- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other

Party that it has received the same and shall forward such request or correspondence to the other Party; and

- (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

34.6.9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Call Off Contract and shall:

- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
- (b) implement any measures necessary to restore the security of any compromised Personal Data;
- (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
- (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

34.6.10. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Call Off Contract as specified in Annex 1 to Call Off Schedule 20 (Authorised Processing Template).


34.6.11. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Call Off Contract which is specified in Annex 1 to Call Off Schedule 20 (Authorised Processing Template).

34.6.12. Notwithstanding the general application of Clause 34.5 of this Call Off Contract, where the Service Provider is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Clause 34.6 of this Call Off Contract."

8.11.4 The existing Clause 34.6 "Malicious Software" of the Call Off Terms shall be renumbered as Clause 34.7 and references within that Clause to Clause 34.6 shall be read as references to Clause 34.7 accordingly.

8.11.5 Call-Off Schedule 20 (Authorised Processing Template) of the Call Off Terms shall be deleted and replaced with the wording set out at Appendix 2 to this Call Off Order Form.

8.12	Alternative and/or Additional Clauses	<i>NOT USED</i>
8.13	<p>Waiver in relation to Customer Roles</p> <p>8.13.1 Notwithstanding the obligations set out in Clause 9 of the Services Schedule (Schedule 2 of the Call Off Terms) (“Checks”) the parties agree that the successful candidate for any Customer role can commence work once the Service Provider has received the following documents:</p> <p>8.13.1.1 Proof of the candidate’s right to work</p> <p>8.13.1.2 Declaration of Interest</p> <p>8.13.1.3 Proof that the Worker has applied for a DBS Check</p> <p>8.13.2 Accordingly, the Customer waives the requirement for the Service Provider to have fully completed the Checks on the Worker, prior to start of the assignment. The Service Provider shall complete the Checks in accordance with the terms of the Call Off Contract as soon as reasonably practical, and no later than 4 weeks after the start of the Worker’s Assignment (“Waiver Period”).</p> <p>8.13.3 The Customer agrees that where the Worker has been permitted to start work, subject to this waiver, such permission is for the duration of the Waiver Period only. In the event that the Service Provider has been unable to complete the Checks and the Customer has not entered into an agreement to extend the Waiver Period, the Service Provider may ask the Worker to stay away from the Customer premises and to cease providing services (“Off-Siting”). For the avoidance of doubt, access to timesheets will be stopped and there will be no obligation to make any payment to the Worker for any work done after Off-Siting.</p> <p>8.13.4 The Customer waives any rights or claims against the Service Provider and/or its sub-contractors in consideration of the supply of Services or Customer Services by the Service Provider in relation to the Worker arising from the Service Provider being unable to complete the Checks on the Worker. The Customer agrees that the Service Provider and its subcontractors will have no liability whatsoever to the Customer or any third party, and further agrees to indemnify the Service Provider in respect of any claim made by any third party, arising as a consequence of the Customer engaging with the Worker prior to completion of the Checks.</p>	
8.14	<p>Waiver in relation to Transition Workers:</p> <p>8.14.1 The Service Provider has previously supplied the workers (listed in Appendix 6) to the Customer pursuant to the terms of a Schedule of Additional Services between the Customer (1), the Department of Health and Social Care “DHSC” (2) and the Service Provider (3), last signed 16th February 2022. Together those workers shall be referred to as the “Transition Workers”.</p> <p>8.14.2 In consideration of the Service Provider entering into the terms of this Call Off Contract, the Customer hereby confirms and agrees that:</p> <p>8.14.2.1 The Customer is satisfied that all Transition Workers have been screened in accordance with its requirements and that all required Checks (including but not limited to any required SC, CTC and DV additional checks) have been completed;</p>	

	<p>8.14.2.2 The Service Provider is not required to undertake any further due diligence in relation to the existing Checks/screening of the Transition Workers referred to at 8.14.2.1; and</p> <p>8.14.2.3 Any requirement for the Service Provider to re-screen any of the Transition Workers in order to comply with its obligations under this Call Off Contract is hereby waived. For the avoidance of doubt, the Service Provider is not required to conduct any screening/Checks in relation to the Transition Workers in connection with their current assignments or any subsequent extension of those assignments (save where requested by the Customer to do so, in writing, on an individual basis).</p>
<p>8.15</p>	<p>ORGANISATIONAL STRUCTURE</p> <p>The attached Organisational Chart shall be followed as the organisational structure used by the Service Provider from the Call Off Commencement Date and, and subject to Clauses 6 and 7 of Appendix 4 hereto, may be varied by the Service Provider, depending on the volume of Services required by the Customer</p> <div style="text-align: center;">  <p>UKHSA governance hierarchy 09.03.22.pp</p> </div>
<p>8.16</p>	<p>INFORMATION</p> <p>Clause 3.2.11 of the Call Off Terms shall be deleted and replaced as follows:</p> <p>3.2.11 all information it provides pursuant to this Call Off Contract (including all information provided by the Service Provider to enable the Customer to complete its Data Protection Impact Assessment and obtain approvals) shall, and it shall procure that all information that the Agency Providers and Workers provide under or in connection with this Call Off Contract shall, at the time of its provision to the Customer be true, accurate, complete and not misleading.</p>

FORMATION OF CALL OFF CONTRACT

BY SIGNING AND RETURNING THIS CALL OFF ORDER FORM (which may be done by electronic means) the Service Provider agrees to enter a Call Off Contract with the Customer to provide the Services in accordance with the Call Off Order Form and the Call Off Terms 10.

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

In accordance with 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 Call Off Order Form from the Service Provider within two (2) Working Days from such receipt.

For and on behalf of the Service Provider:

Name and Title	[REDACTED]
Signature	[REDACTED]
Date	[REDACTED]

For and on behalf of the Customer:

Name and Title	[REDACTED]
Signature	[REDACTED]
Date	[REDACTED]

APPENDIX 1: NOT USED

APPENDIX 2: Call-Off Schedule 20

Appendix 2, Annex 1 : Authorised Processing Template

1. The contract details of the Customer Data Protection Officer is:
[REDACTED] data.protection@dhsc.gov.uk
2. The contract details of the Service Provider Data Protection Officer is:
[REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Contract Reference:	C70860
Date:	1st April 2022
Description Of Authorised Processing	The purpose of processing by the Service Provider is to source and deliver appropriate contingent worker resources to the Customer. The data to be processed is covered under "Type of Personal Data"
Identity of the Controller for each Category of Personal Data	<p>The Customer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> ● Personal Data Processed specifically for performing Baseline Personnel Security Standard (BPSS) screening ● Personal Data processed in relation to drug and alcohol screening <p>The Parties are Joint Controllers</p> <p>The Parties acknowledge that they are not Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p>If the circumstances change so that the Parties would be considered Joint Controllers for the purposes of the Data Protection Legislation then the parties agree to vary the contract in accordance with the Variation Procedure and update this Schedule with the following details</p> <ul style="list-style-type: none"> ● The scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together <p>The parties acknowledge should at any point the parties be determined as Joint Controllers, Annex 2 : Joint Controller Agreement attached to this Schedule will apply to that processing.</p>

	<p>The Parties are Independent Controllers of Personal Data</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of all Services provided by the Service Provider to the Customer under the Call Off Contract. The Parties acknowledge and agree that the Data Sharing Agreement attached as Annex 3 to this Schedule will apply in respect of this processing as Independent Controllers of the Personal Data.</p>
<p>Subject matter of the processing</p>	<ul style="list-style-type: none"> • Performing BPSS screening on behalf of the Customer. • Processing drug and alcohol related screening data on behalf of the Customer. <p>Note that for some Personal Data processed as part of the BPSS screening, the Service Provider has their own lawful basis of processing and is neither a Processor on behalf of the Customer nor a Joint Controller but rather an independent Controller.</p>
<p>Duration of the processing</p>	<p>From the outset of the Call-Off Contract start date (of 1st April 2022) and up to 7 years after the last Worker finishes their assignment in order to meet legal obligations.</p>
<p>Data Processing Locations</p>	<p>Data Processing locations are set out in the DPIA.</p> <p>The services will be delivered from the following locations: -</p> <ul style="list-style-type: none"> - Krakow (Puzkarska 7F) - Belfast (Millenium House, Great Victoria Street) - London (AMS Office, 7 Bishopsgate) - Client sites (Various Contracting Customer Locations UK wide) - Home Workers (Various AMS Employee Home Locations) <p>The systems used by the Service Provider have various storage locations as follows:</p> <ul style="list-style-type: none"> - Germany - Netherlands - Ireland - UK
<p>Nature and purposes of the processing</p>	<p><i>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.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc</i></p>

	<p>For both BPSS and drug and alcohol screening, providing the information to the Customer for the purpose of fulfilling its obligations under the Framework Agreement.</p> <p>For BPSS, specifically the collection of Personal Data from the Data Subject including proof of name, proof of date of birth, proof of employment / academic history, proof of national insurance number, proof of address, proof of right to work, proof of signature, and a criminal record check result which are then validated against the BPSS screening requirements. The result of the BPSS check is provided to the customer, and records are retained in line with the retention policy.</p> <p>Note that some of the records processed for BPSS are also processed for the Service Providers purposes, not under the control of the Customer.</p> <p>For drug and alcohol screening, the collection of Personal Data from the Data Subject, the sharing of the Personal Data with a third party provider selected by the Customer for the purposes of performing drug and alcohol screening, receiving the result of the test (pass or fail only), sharing the result with the Customer, and records are retained in line with the Customers/Service Provider’s retention policy.</p>
Type of Personal Data	<p>All contingent workers</p> <p>Full name</p> <p>Address</p> <p>Postcode</p> <p>Mobile/Home Telephone number</p> <p>Photo</p> <p>Email address</p> <p>Nationality/immigration status</p> <p>Bank details</p> <p>Job title</p> <p>Employment records</p> <p>Proof of right to work</p> <p>Proof of date of birth</p> <p>Proof of national insurance</p> <p>Proof of signature</p> <p>Proof of address</p> <p>Work and/or education history</p> <p>Criminal record check result</p> <p>Drug and alcohol test results (pass or fail only)</p>
Categories of Data Subject	Contingent Workers

Approved subcontractors	Access Screening
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	The Personal Data will be retained for each hired Worker for up to 7 years after the last payment is made in relation to the assignment performed. For those Worker applicants not engaged the Personal Data will be retained only as long as is necessary to fulfil the purposes identified in the data protection statement. Typically this is 12 months for screening data.

Appendix 2, ANNEX 2: Joint Controller Status and Allocation of Responsibilities

- 1.1 With respect to Personal Data which has been identified in Annex 1 as under Joint Control of the Parties because it is envisaged that they shall jointly determine the purpose and means of processing and each be a Data Controller in respect of that Personal Data. Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Joint Data Controllers.
- 1.2 The Parties agree that the Service Provider
 - (a) shall be the Exclusive Point of Contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR.
 - (b) shall direct Data Subjects to the Exclusive Point of Contact's Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
 - (c) shall be solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR; and
 - (d) shall make available to Data Subjects the essence of this Schedule (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as Exclusive Point of Contact. This must be outlined in the Exclusive Point of Contact's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).
- 1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.
2. The Joint Controllers each undertake that they shall:
 - (a) report to the other Party every three months on:
 - (i) the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
 - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
 - (iii) 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;
 - (iv) any communications from the Information Commissioner or any other regulatory Customer in connection with Personal Data; and
 - (v) 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 Personal Data under Joint Control during that period;

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1 (a)(i) to (v); and
- (c) 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.
- (d) obtain the consent of Data Subjects or carrying out and documenting legitimate interest assessments, in accordance with the GDPR, for all Processing;
- (e) 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 this Agreement or is required by Law). For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex 2
- (f) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information.
- (g) 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.
- (h) 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:
 - (i) are aware of and comply with their duties under this Annex 2 (*Joint Controller Agreement*) and those in respect of Confidential Information
 - (ii) 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;
 - (iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;
- (i) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
 - (i) nature of the Personal 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.
 - (j) 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 Contractor holds; and
 - (i) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach
- 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 the it's 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 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:
- (a) 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 Legislations;
 - (b) all reasonable assistance, including:
 - (i) 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;
 - (ii) 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;
 - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;
 - (iv) 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 been lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it was that Party's own Personal 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 upon becoming aware of the Personal Data Breach relating to the Personal Data Breach, in particular:

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Service Provider's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 Subject to Clause 21.3 of the Call Off Terms and subject to the Service Provider's rights in respect of Confidential Information, the Service Provider shall permit:

- (a) the Customer or its Auditor, to conduct, at the Customer'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 Customer, or a third-party auditor acting under the Customer's direction, reasonable access to premises controlled by the Service Provider 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 UK GDPR by the Service Provider so far as relevant to the Call Off Contract, and procedures, The Customer may, in its sole discretion, require the Service Provider to provide evidence of the Service Provider's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

- a) provide all reasonable assistance to each other in preparing any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures);
- b) maintain full and complete records of all processing carried out in respect of the Personal Data in connection with this Call Off Contract, in accordance with the terms of Article 30 UK GDPR , such records shall include the following information:
 - i. the categories and purposes of processing carried out in respect of the Personal Data;
 - ii. where applicable, complete information about transfers of Personal Data outside the EU, and the safeguards implemented in respect of such transfers necessary to comply with Law;
 - iii. a general description of the Protective Measures which the Provider has implemented to safeguard the Personal Data in accordance with this

clause and in compliance with Data Protection Legislations and ICO Guidance

6. The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Customer may on not less than thirty (30) Working Days' notice to the Service Provider and subject to agreement with the Service Provider (such agreement not to be unreasonably withheld) amend the Call Off 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 Joint Controller for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- a) if in the view of the Information Commissioner, the Customer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Customer, its employees, agents, contractors (other than the Contractor) or systems and procedures controlled by the Authority/Customer, then the Authority/Customer shall be responsible for the payment of such Financial Penalties. In this case, the Authority/Customer 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 Service Provider shall provide to the Authority/Customer and its third party investigators and auditors, on request and at the Authority's/Customer's reasonable cost, full cooperation and access to conduct a thorough audit of Personal Data Breach;
- b) if in the view of the Information Commissioner, the Service Provider is responsible for the Personal Data Breach, in that it is not a breach that the Authority/Customer is responsible for, then the Service Provider shall be responsible for the payment of these Financial Penalties. The Authority/Customer will provide to the Service Provider and its auditors, on request and at the Service Provider's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach.
- c) If responsibility is unclear, then the Joint Controllers 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 Dispute Resolution.

7.2 If any of the Joint Controllers is the defendant in a legal claim brought 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 a court of competent jurisdiction or the Information Commissioner to be responsible for the Personal Data Breach shall be liable for the losses arising from such breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court or the Information Commissioner, as the case may be.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

- a) the Party responsible for the relevant breach shall be responsible for the Claim Losses; and
- b) if responsibility is unclear, then the Parties shall be responsible for the Claim Losses equally.

Nothing in either clause 7.2 or clause 7.3 shall preclude the Parties 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 Customer.

8. Termination

8.1 If the Service Provider is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Customer shall be entitled to terminate the Call Off Contract in accordance with Clause 41 of the Call Off Terms.

9. Sub-Processing

9.1 In respect of any Processing of Personal Data under Joint Control by a sub-contractor or agents of a Party, each Party shall:

- (a) carry out adequate due diligence on such third party or the sub-contractor to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Call Off Contract and provide evidence of such due diligence to the other Party where reasonably requested by the other Party or the Information Commissioner; and
- (b) ensure that a suitable agreement is in place with the third party or the Sub-contractor or Key Sub-contractor including as may be required under applicable Data Protection Legislation.

10. Data Retention

10.1 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 appropriate 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 Party for statutory compliance purposes or as otherwise required by this Agreement), and taking all further actions as may be necessary or desirable to ensure its compliance with Data Protection Legislation and its privacy policy.

Appendix 2, Annex 3: Data sharing agreement – Independent Controllers (Controller to Controller) (UK GDPR and DPA 2018)

Recitals:

A)The provisions of this Annex 3 together with its Schedules (together, the “Data Sharing Agreement”) are intended to be supplemental to new Clause 34.6 of the Call Off Terms as inserted by Clause 8.11.3 of the Call Off Order Form.

B)The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of all Services provided by the Service Provider to the Customer under the Call Off Contract as set out at Annex 1 of Schedule 20 to the Call Off Terms (Authorised Processing Template).

C)The Parties acknowledge and agree that the Data Sharing Agreement will apply in respect of this processing as Independent Controllers of the Personal Data.

AGREED TERMS

1. Interpretation

The following definitions and rules of interpretation apply in this Data Sharing Agreement.

1.1 Definitions:

Agreed Purpose: has the meaning given to it in clause 2 of this Data Sharing Agreement.

Criminal Offence Data: means Personal Data relating to criminal convictions and offences or related security measures to be read in accordance with section 11(2) of the DPA 2018 (or other applicable Data Protection Legislation)

Deletion Procedure: has the meaning given to it in clause 8.3 and Schedule 3 to this Agreement.

Data Sharing Code: the Information Commissioner's Data Sharing Code of Practice which came into force on 5 October 2021, as updated or amended from time to time.

Data Subject Access Request: the exercise by a data subject of his or her rights under Article 15 of the UK GDPR.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including:

- i. the UK General Data Protection Regulation ;the Data Protection Act 2018 and regulations made thereunder) ;
- ii. and the Privacy and Electronic Communications Regulations 2003 as amended;
- iii. any all-other legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and

- iv. the guidance and codes of practice issued by the Information Commissioner or other relevant data protection or supervisory authority and applicable to a Party.

Shared Personal Data: the Personal Data and Special Categories of Personal Data to be shared between the Parties under clause 2 of this Agreement.

Special Categories of Personal Data: the categories of Personal Data set out in Article 9(1) of the UK GDPR.

Supervisory Authority: The Information Commissioner.

Term: The Initial Call Off Period and any subsequent Call Off Extension Period

- 1.2 **Controller, Processor, Data Subject and Personal Data, Processing, Personal Data Breach and "appropriate technical and organisational measures"** shall have the meanings given to them in the Data Protection Legislation.
- 1.3 In the case of any ambiguity between any provision contained in the body of this Data Sharing Agreement and any provision contained in the Schedules or appendices to the Data Sharing Agreement, the provision in the body of this Data Sharing Agreement shall take precedence.
- 1.4 Unless the context otherwise requires, any reference to European Union law that is directly applicable or directly effective in the UK at any time is a reference to it as it applies in England and Wales from time to time including as retained, amended, extended, or re-enacted or otherwise given effect by the EU (Withdrawal) Act 2018.
- 1.5 A reference to **writing** or **written** includes email.
- 1.6 Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.

2. Purpose

- 2.1 This Data Sharing Agreement sets out the framework for the sharing of **Personal Data** on the basis of one **Controller** sharing Personal Data with another **Controller**, and where each Controller is acting independently. It defines the basis on which the Parties consider it lawful and necessary to share the Shared Personal Data, as well as the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.
- 2.2 The Parties consider data sharing to be necessary for the purpose of the Service Provider delivering and managing appropriate contingent worker resources to the Customer.
- 2.3 The Parties agree to only Process Shared Personal Data, as described in Schedule 2.

- 2.4 The Parties shall not process Shared Personal Data in a way that is incompatible with the purposes described in this clause 2 (**Agreed Purpose**).
- 2.5 Each Party shall appoint a single point of contact (**SPoC**) who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative. The points of contact for each of the Parties are:
- (a) The office of the Data Protection Officer DPO at UKHSA (data_protection@dhsc.gov.uk)
 - (b) [REDACTED]
- 2.6 Under this Agreement, when one Party transfers its data to the other Party the terms of this Agreement shall apply.

3. Compliance with the Data Protection Legislation

- 3.1 Each Party must ensure compliance with the Data Protection Legislation at all times during the Term.
- 3.2 Each Party enters into this Data Sharing Agreement on the basis that it has such valid registrations and paid such fees as are required by its Supervisory Authority which, by the time that the data sharing is expected to commence, covers the intended data sharing pursuant to this Data Sharing Agreement, unless an exemption applies.

4. Shared Personal Data

- 4.1 The types of Personal Data including Special Categories of Personal Data shared between the Parties is listed in Schedule 2.
- 4.2 The Parties agree that the Shared Personal Data is not irrelevant, unnecessary or excessive with regard to the Agreed Purposes.

5. Lawful, fair and transparent processing

- 5.1 Each Party shall ensure that it Processes the Shared Personal Data fairly, transparently and lawfully during the Term
- 5.2 Each Party agrees that the legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal Data for the Agreed Purpose are documented within a DPIA.

6. Data quality

- 6.1 The Parties shall take all reasonable steps to ensure that before the Service Commencement Date the Shared Personal Data is accurate and will update the same if reasonably required prior to transferring the Shared Personal Data.
- 6.2 Shared Personal Data must be limited to the Personal Data described in Schedule 2.

7. Data Subjects' rights

- 7.1 The Parties each agree to provide such assistance as is reasonably required to enable the other Party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.
- 7.2 The SPoC for each Party is responsible for maintaining a record of individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The SPoC for each Party are detailed in clause 2.5.

8. Data retention and deletion

- 8.1 The Parties shall not retain or Process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes. This should be no longer than is necessary to carry out the Agreed Purpose.
- 8.2 Notwithstanding clause 8.1, the Parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and/or industry.
- 8.3 Each Party shall ensure that any Shared Personal Data is returned to each Party or destroyed in accordance with the agreed Deletion Procedure set out in Schedule 3 in the following circumstances:
- (a) on expiry of the Term;
 - (b) once Processing of the Shared Personal Data is no longer necessary for the purposes it was originally shared for, as set out in clause 2.
- 8.4 Following the deletion of Shared Personal Data in accordance with clause 8.3, each Party shall notify the other Party that the Shared Personal Data in question has been deleted in accordance with the Deletion Procedure in Schedule 3 to this Agreement.

9. Transfers

- 9.1 For the purposes of this clause, transfers of Personal Data shall mean any sharing of Personal Data by the Customer or the Service Provider with a third party, and shall include, but is not limited to, the following:
- (a) subcontracting the Processing of Shared Personal Data;
- 9.2 If either Party appoints a third party Processor to Process the Shared Personal Data it shall comply with Articles 28 and 30 of the UK GDPR and shall remain liable to the other Party for the acts and/or omissions of the Processor.
- 9.3 Neither Party shall disclose or transfer Shared Personal Data outside the EEA.

10. Security and training

- 10.1 Each Party shall only provide the Shared Personal Data to the other Party by using secure methods as agreed in the Security Management Plan.
- 10.2 The Parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:
- (a) prevent:
 - (i) unauthorised or unlawful Processing of the Shared Personal Data; and
 - (ii) the accidental loss or destruction of, or damage to, the Shared Personal Data.
 - (b) ensure a level of security appropriate to:
 - (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
 - (ii) the nature of the Shared Personal Data to be protected.
- 10.3 The level of technical and organisational measures agreed by the Parties as appropriate as at the Service Commencement Date, having regard to the state of technological development and the cost of implementing such measures is set out in the Security Management Plan. The Parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the Term.
- 10.4 It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and Process the Shared Personal Data in accordance with the technical and organisational security measures set out in the Security Management Plan, together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the processing of Personal Data.

- 10.5 The level, content and regularity of training referred to in clause 10.4 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and Processing of the Shared Personal Data.

11. Personal data breaches and reporting procedures

- 11.1 Each Party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) Data Subjects under Articles 33 and 34 of the UK GDPR and shall inform the other Party of any Personal Data Breach irrespective of whether there is a requirement to notify the Supervisory Authority or Data Subject(s).
- 11.2 The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

12. Review and termination of Agreement

- 12.1 The Parties shall review the effectiveness of this data sharing initiative every six months as agreed between parties, having consideration to the aims and purposes set out in clause 2.2 and clause 2.3. The Parties shall continue, amend or terminate the Agreement depending on the outcome of this review.
- 12.2 The review of the effectiveness of the data sharing initiative will involve:
- (a) assessing whether the purposes for which the Shared Personal Data is being Processed are still the ones listed in clause 2 of this Agreement;
 - (b) assessing whether the Shared Personal Data is still as listed in clause **4.1** and **Error! Bookmark not defined.Error! Reference source not found.** of this Agreement;
 - (c) assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and
 - (d) assessing whether Personal Data Breaches involving the Shared Personal Data have been handled in accordance with this Agreement and the applicable legal framework.
- 12.3 Each Party reserves its rights to inspect the other Parties arrangements for the Processing of Shared Personal Data and to terminate the Agreement where it considers that the other Party is not Processing the Shared Personal Data in accordance with this Agreement.

13. Resolution of disputes with data subjects or the Supervisory Authority

- 13.1 In the event of a dispute or claim brought by a Data Subject or the Supervisory Authority concerning the Processing of Shared Personal Data against either or both

Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

- 13.2 The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Supervisory Authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- 13.3 Each Party shall abide by a decision of a competent court of England and Wales or of the Supervisory Authority.

14. Warranties

- 14.1 Each Party warrants and undertakes that it will:
- (a) Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations;
 - (b) On request, make available to the Data Subjects who are third party beneficiaries a copy of this Data Sharing Agreement, unless the Data Sharing Agreement contains confidential information;
 - (c) Respond within a reasonable time and as far as reasonably possible to enquiries from the relevant Supervisory Authority in relation to the Shared Personal Data;
 - (d) Respond to Subject Access Requests in accordance with the Data Protection Legislation;
 - (e) Where applicable, maintain registration with all relevant Supervisory Authorities to Process all Shared Personal Data for the Agreed Purpose; and
 - (f) Take all appropriate steps to ensure compliance with the security measures set out in clause 10 above.
- 14.2 Service Provider warrants and undertakes that it will not disclose or transfer the Shared Personal Data outside the EEA
- 14.3 Except as expressly stated in this Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

15. Indemnity

- 15.1 Subject to Clause 36 of the Call Off Terms, UKHSA and the Service Provider undertake to indemnify each other and hold each other harmless from any cost, claims, charge, damages, expense (including but not limited to reasonable legal costs) or loss, actions

and proceedings which they cause each other as a result of their breach of any of the provisions of this Data Sharing Agreement,.

15.2 Indemnification hereunder is contingent upon:

- (a) the Party to be indemnified (the **indemnified Party**) promptly notifying the other Party) (the **indemnifying Party**) of a claim;
- (b) the indemnifying Party having sole control of the defence and settlement of any such claim; and
- (c) the indemnified Party providing reasonable co-operation and assistance to the indemnifying Party in defence of such claim.

16. Allocation of cost


Each Party shall perform its obligations under this Data Sharing Agreement at its own cost.

Schedule 1 KEY LEGISLATIVE PROVISIONS AND AUTHORITATIVE GUIDANCE

- The Data Protection Legislation

Schedule 2 Shared Data and Personal Data

Description	Details
Categories of Data Subjects	AMS Staff, Candidates, Customer Staff, Contractors, Relatives of data subjects, Suppliers
Type of Data (including Personally Data and Special Categories of Personal Data)	Education, Employee HR Details, Employee Performance ,Employee Travel & Expense ,Family & Social Circumstances, Financial, Health & Welfare, Identification Checks & Background Vetting, Personal, Professional Experience & Affiliations Physical / Mental Health or Condition
Nature and purposes of Processing	<p>The Public Sector Resourcing (PSR) service being implemented and delivered to Crown Commercial Services (CCS) is intended to deliver a contingent workforce management solution, using technology to underpin the services. The service will include the contingent worker sourcing, through onboarding, contract management, supply chain management, exit management, and associated reporting and production of management information. Additional projects may be implemented from time to time as necessary to deliver change, such as legislative change or continual improvement.</p> <p>AMS purpose of processing is to deliver and manage appropriate contingent worker resources for the Contracting Authorities.</p> <p>In order to deliver the services, the personal data of contingent workers, client staff, AMS staff, and supplier staff will need to be processed.</p> <p>This information will be held within systems and transferred between them through a number of different mechanisms including automated and manual, and also protected through encryption, and in some circumstances unencrypted.</p>
Lawful grounds/basis for sharing the data	<p>GDPR: For processing personal data of applicants and successful applicants: GDPR Article 6 (1) (b) – “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract” GDPR Article 6 (1) (c) – “processing is necessary for compliance with a legal obligation to which the controller is subject” GDPR Article 6 (1) (f) - "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and</p>

	<p>freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."</p> <p>For processing special category data of applicants and successful applicants (reasonable adjustments for selection process and also while on assignment):</p> <p>GDPR Article 9 (2) (b) – “processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment”</p> <p>Pre-employment screening to HMG Baseline Personnel Security Standard (BPSS)</p> <p>In accordance with HMG’s Baseline Personnel Security Standard (BPSS)</p> <p>https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.</p> <p>GDPR Article 6 (1) (e) – “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”</p> <p>GDPR Article 9 (2) (b) – “processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment”</p> <p>Data Protection Act 2018 (DPA 2018):</p> <p>Schedule 1, Part 1, 1 – Employment, social security and social protection</p> <p>1 (1) This condition is met if— (a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment</p> <p>Schedule 1, Part 2, 2 - (1) This condition is met if the processing is necessary for health or social care purposes.</p> <p>(2) In this paragraph “health or social care purposes” means the purposes of—(b) the assessment of the working capacity of an employee.</p>
Privacy Notice	Not included in this agreement
DHSC DPO Details	<p>Office of The Data Protection Officer at DHSC</p> <p>data_protection@dhsc.gov.uk</p> <p>Department of Health and Social Care</p> <p>1st Floor North</p> <p>39 Victoria Street</p> <p>London SW1H 0EU</p> <p>Z5571792</p>
Privacy Notice	
DPO details	<p></p> <p>ICO registration: Z6924746</p>
Consenting process if applicable	Not applicable
Processor / Sub-Processor	Broadbean

	Access Group SAP - Fieldglass NQC Marketplace
Onward data sharing	As per above
Data Flow Diagram	Not included due to complexity – details contained in PSR DPIA and can be provided on request
File type	
Frequency of Transfer	Ongoing basis during the term of the agreement
Transfer mechanism	Automated and manual processes
Data will be stored	Yes
Duration of Processing	Ongoing for the duration of the agreement
Plan for return or destruction of Personal Data upon termination of the Agreement	Automated or manual deletion of data where no lawful basis to retain the data remains

Schedule 3 Deletion procedure

A data destruction certificate must be used to notify UKHSA of the destruction of the Shared Data and Personal Data. The UKHSA Certificate of Data Destructions template (below) should be completed and returned to UKHSA to confirm deletion procedures, **if applicable to this agreement.**

The terms of this Data Sharing Agreement require confirmation that all the physical and logical data detailed on a data destruction certificate has been destroyed, including the original data and any copies in whole or in part.

The following standards and guidelines are the minimum basis for data decommissioning or destruction:

National Cyber Security Centre (NCSC) guidance on end-user device reset procedures:

<https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning>

NCSC guidance on secure sanitisation of storage media: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>



Certificate of Data Destruction

This certificate is issued to confirm the destruction of the described data between the parties.

Issuing Project / Function	
Project Title / Function Name:	
Reference (If Any):	
Receiving Organisation / Parties:	
List Data mart / Data sets:	

Receiving Organisation	
Principal Contact:	
Principal Contact Job Role:	
Receiving Organisation Registered Name:	
Organisation Full Registered Address:	
Organisation Relationship with UKHSA: E.g. Controller to controller. Controller to processor etc	

Data Destruction Details			
Data Format: E.g. Soft copy/Hard copy		Size:	
Method of Destruction:		Date Destroyed:	
Evidence of Destruction: E.g. Script log, screenshot etc		Destroyed By:	
Please describe steps taken to put data beyond use. (e.g. for cloud storage) Please see ICO link for guidance			
Additional Information:			

We / I confirm that all destruction of the data has been carried out using appropriate secure methods to the format and security of the data, whilst preserving the confidentiality of the data.

We / I confirm that all back-up copies, security copies, preservation copies, duplicate copies and any other available copies will be put permanently beyond use and it is irretrievable by any means.

Signed:	Date:
Print Full Name:	
Job Role:	

APPENDIX 3 – PERFORMANCE REPORTING AND MONITORING (GOVERNANCE PACK)



Appendix 3 UKHSA
governance pack FIN/

APPENDIX 4: SCHEDULE OF ADDITIONAL SERVICES

Unless otherwise terminated in accordance with paragraphs 9 and 10 below, the Service Provider shall provide the additional services set out in this Appendix 4 ("**Customer Services**") for the duration of the Call Off Contract.

Customer Services

- 1 The Service Provider will provide to the Customer a team of 10 (ten) Service Provider Personnel, to:
 - 1.1 support and guide Hiring Managers in legacy test and trace teams, guiding them through the end to end recruitment process (save that the Hiring Managers will make the final decision in selection of successful candidates);
 - 1.2 manage all aspects of the Hiring Managers' responsibilities in Fieldglass;
 - 1.3 liaise with PSR support teams;
 - 1.4 minimise the administrative burden for Hiring Managers associated with the recruitment and on-boarding of new starters into the Customer.

Customer dependencies

2. The Customer will:
 - 2.1 provide a list of vacancies, hiring manager details, Vacancy Control Committee (VCC) number, Job title and any other relevant information which will support hiring activity.
 - 2.2 provide an Executive Sponsor within the Customer programme who has authority to make decisions and can escalate accordingly to Chief People Officer.
 - 2.3 verify the declaration of interest referenced in clause 8.13.1.2 of the Call Off Order Form (verified by Customer HR) and share with Service Provider.

Charges and invoicing

- 3 The Customer will pay the Service Provider a monthly management fee of £66,066 excluding VAT for providing the Customer Services ("**Customer Charges**") and for the avoidance of doubt the Customer Charges are payable in addition to the Call-Off Contract Charges due for any Workers successfully hired.
- 4 The Service Provider shall invoice the Customer Charges monthly in advance.
- 5 The Customer shall pay the Customer Charges properly due and payable to the Service Provider in cleared funds within thirty (30) days of receipt of a Valid Invoice, submitted to the address specified by the Customer in the Call Off Order Form.

Changes in volumes or requirements

- 6 Should the parties agree that increased support is required or where notice of reduced support is given in accordance with this clause, the revised resources will be charged on a per head basis according to the rate card in the Table below, subject to the Customer providing the Service Provider with a minimum of two (2) weeks written notice of any request to increase or reduce any resources. The same calculation shall be applied if the service is terminated early.
- 7 The Customer acknowledges that should the parties wish to change the composition of the on-site team (for example, a different combination of role types), this will necessitate a review of the Customer Charges and may lead to an increase in those charges. Any such change in composition and charges will however be subject to the prior written agreement of the parties.

	Role	Daily Rate (Exc. VAT)
<i>Resource 1</i>	<i>Recruitment Admin Specialist</i>	■■■
<i>Resource 2</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 3</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 4</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 5</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 6</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 7</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 8</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 9</i>	<i>Resourcing Team Lead</i>	■■■
<i>Resource 10</i>	<i>Resourcing Team Lead</i>	■■■

Termination

- 9 The Customer and the Service Provider shall have the right to terminate this Schedule of Additional Services for convenience by issuing a Termination Notice to the other giving at least two (2) weeks' notice subject to such notice not being served before 30th April 2022;
- 10 This Schedule of Additional Services shall terminate automatically on termination of the Call Off Contract.

Definitions

- 11 Words and expressions in this Schedule of Additional Services shall have the meanings given to them in the Call Off Contract unless otherwise defined here.

APPENDIX 5: PSR SECURITY MANAGEMENT PLAN



AMS_Security_Management_Plan_v_1.5.doc

APPENDIX 6: TRANSITION WORKERS



Appendix 6
Transition Workers