Crown
Commercial
Service
Supplier

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Contents

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	196577664306413
Call-Off Contract reference	6GBR212-332620-405309
Call-Off Contract title	UK Heath Security Agency (UKHSA) Implementation Services
Call-Off Contract description	A managed transformation and migration services to driving cost effective and repeatable process for merging or divesting collaboration environments for organisations. Supplier will develop a plan which supports a predictable path to achieve Buyers strategic goals for change and Microsoft's migration approach places emphasis on minimizing impact to users.
Start date	17/05/2021
Expiry date	16/05/2022
Call-Off Contract value	£1,514,415.40
Charging method	Time & Materials / Fixed Fee
Purchase order number	TBC

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	The Secretary of State for Health and Social Care acting as part of the Crown Through: **Public Health England** Wellington House London SE1 8UG
To the Supplier	Microsoft Limited Microsoft MCS – Public Sector, Building 1 Microsoft Campus, Thames Valley Park, Reading, RG6 1WG
Together the 'Parties'	

Principle contact details

For the Buyer:

Title: [redacted]

Name: [redacted]

Email: [redacted] Phone: [redacted]

For the Supplier:

Title: [redacted]

Name: [redacted]

Email: [redacted]

Phone: 07957493853

Call-Off Contract term

Start date	This Call-Off Contract Starts on **17/05/2021** and is valid for **12 months**
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 1 month written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot	This Call-Off Contract is for the provision of Services under: Lot 3: Cloud support
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined in the statement of Work as referenced in Schedule 1 'Services'.

Additional Services Location	The Services will be delivered remotely from the Supplier's premises and there will be no onsite working at the Buyer's premises during the COVID-19 pandemic unless it is safe to do so, and where it has been agreed between the Parties and is reasonably required for the provision of the Services.

Quality Standards	The quality standards required for this Call-Off Contract are detailed in the Statement of Work.
Technical Standards	The technical standards used as a requirement for this Call-Off Contract are detailed in the Statement of Work.
Service level agreement	Service level and availability criteria for this Call-Off Contract are not applicable.
Onboarding	The onboarding plan (if any) for this Call-Off Contract shall be described in the Statement of Work.
Offboarding	The offboarding plan (if any) for this Call-Off Contract shall be described in the Statement of Work.
Collaboration	In accordance with this Call-off Contract, the Buyer does not require the Supplier to enter into a Collaboration Agreement.
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed 100% of the charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for Buyer Data Defaults will not exceed 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other Defaults will not exceed 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.

Insurance	The insurance(s) required will be: • a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract. • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law. The Supplier may, in its sole discretion, fulfil its insurance obligations described herein via commercial insurance, excess insurance, a program of self-insurance or a combination of any of the aforementioned options. For the avoidance of doubt and notwithstanding anything to the contrary, the Supplier is under no obligation to provide the following to demonstrate compliance of its insurance obligations; (1) receipts for insurance premium, or (2) evidence of payment of the latest premiums due.
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 60 consecutive days.
Audit	Not applicable
Buyers responsibilities	The Buyer`s responsibilities shall be defined in the Statement of Work.
Buyers equipment	The Buyer’s equipment to be used with this Call-Off Contract Shall be defined in the Statement of Work.

Supplier’s information

Subcontractors or partners	The following is a list of the Supplier’s Subcontractors or Partners: - Currently n/a Supplier may also rely on the services of other entities in the global Microsoft group of companies in providing the Services, to which the Buyer hereby consents.

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is BACS.
Payment profile	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to: Accounts Payable, [redacted] and CC in [redacted]
Invoice information required	All invoices must include: All invoices must include Purchase Order (PO) and the project reference number.
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-off Contract value	The total value of this Call-Off Contract is £1,514,415.40
Call-Off Contract charges	The breakdown of the Charges is detailed in Schedule 2 below.

Additional Buyer terms

Performance of the Service and Deliverables	As defined in the Statement of Work.
Guarantee	Not applicable.
Warranties representations	Incorporated Framework Agreement clause 4.1 only.
Supplemental requirements in addition to the Call-Off terms	Not applicable.
Alternative clauses	Not applicable.

Buyer specific amendments to/refinements of the Call-off Contract terms	Confidentiality: Nothing in the Framework Agreement or this Call-Off Contract will prevent either party from disclosing the other party's Confidential Information to its employees, Affiliates*, contractors, advisors and consultants ("Representatives") and then only on a need-to-know basis under nondisclosure obligations at least as protective as the Framework Agreement and this Call-Off Contract. Each party remains responsible for the use of the other party's Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party. A party may disclose the other's Confidential Information if required by law; but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order. *"Affiliate" means any legal entity that controls, is controlled by, or that is under common control with a party. „Control" means ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity. Intellectual Property Rights:

	• The Buyer and the Supplier explicitly agree that the IPRs under this Call-Off Contract are not suitable for publication as open source, unless the parties mutually agree on a case by case basis to such publication. • For the avoidance of doubt the Buyer and the Supplier explicitly agree that „the Buyer`s ordinary business activities“ means Buyer`s internal business use. • The Buyer and the Supplier explicitly agree as follows: Defense of third party claims. The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information, and authority, and must take all reasonable action to mitigate its losses arising from the third-party claim. The defending party will reimburse the other party for reasonable out-ofpocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims. a) By Microsoft. Microsoft will defend Buyer against any third-party claim to the extent it alleges that a Product, Fix or Services Deliverable made available by Microsoft for a fee and used within the scope of the license granted (unmodified from the form provided by Microsoft and not combined with anything else) misappropriates a trade secret or directly infringes a patent, copyright, trademark or other proprietary right of a third party. If Microsoft is unable to resolve a claim of infringement under commercially reasonable terms, it may, at its option, either (1) modify or replace the Product, Fix or Services Deliverable with a functional equivalent; or (2) terminate Buyer's license and refund any prepaid license fees (less depreciation on a five-year, straightline basis) for perpetual licenses and any amount paid for Online Services for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Buyer's continued use of a Product, Fix, or Services Deliverable after being notified to stop due to a third-party claim. b) By Buyer. To the extent permitted by applicable law, Buyer will defend Microsoft against any third-party

	claim to the extent it alleges that: (1) any Buyer Data or non-Microsoft software hosted in an Online

Service by Microsoft on Buyer's behalf misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (2) Buyer’s use of any Product, Fix, or Services Deliverable alone or in combination with anything else, violates the law or damages a third party.

No limitation or exclusions will apply to liability arising out of either party’s (1) confidentiality obligations (except for all liability related to Buyer Data which will remain subject to the limitations above); (2) defense obligations; or (3) violation of the other party’s intellectual property rights.

The Microsoft Professional Services Data Protection Addendum (as attached) is hereby incorporated into this CallOff Contract. Notwithstanding incorporated Framework clause 8.3 and clause 8.3 of the Framework Agreement, the parties explicitly agree as follows:

a) for the purposes of Paragraph 5(d) of Schedule 4 of the Framework Agreement as incorporated into this Call-Off Contract via incorporated Framework clause 8.59 (or any equivalent requirement for consent for the transfer of Personal Data incorporated into the Framework Agreement or this Call-Off Contract following the date of this Call-Off Contract), the Buyer hereby consents to the transfer of Personal Data in accordance with the Personal Data transfer principles and details set out in the MPSDPA;

b) for the purposes of incorporated Framework clause 8.35 and Paragraph 12(a) and 12(b) of Schedule 4 of the Framework Agreement as incorporated into this Call-Off Contract via incorporated Framework clause 8.59 (or any equivalent provision that is incorporated into the Framework Agreement or this Call-Off Contract following the date of this Call-Off Contract):

    i. the Buyer hereby confirms that, prior to the execution of this Call-Off Contract, it has been provided with details of the Subprocessors that the Supplier will use in connection with the Processing carried out pursuant to this Call-Off Contract;

    ii. the Buyer hereby gives its prior written consent to the use of such Sub-processors by the Supplier; and

	iii. where any additional or replacement Subprocessors are to process any Personal Data following the execution of this Call-Off

	Contract, the parties agree that the process for the approval of additional or replacement Sub-processors set out in the MPSDPA shall apply.
Public Services Network (PSN)	For the purposes of this Call-Off Contract the Public Services Network (PSN) is not being utilised.
Personal Data and Data Subjects	The Microsoft Professional Services Data Protection Addendum, as incorporated into this Call-Off Contract, shall apply.

1. Formation of contract

1.1. By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2. The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3. This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4. In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	Buyer
Name	[redacted]	[redacted]
Title	[redacted]	[redacted]
Signature	[redacted] Rob Sillitoe (May 14, 2021 09:17 GMT+1)	[redacted]
Date	May 14, 2021	May 14, 2021

Schedule 1: Services

Microsoft will perform the work described in the Statement of Work:

- Merger, Acquisition, Divestiture Migration for Modern Work and WVD, 08/05/2021, 4.0

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Microsoft 365 Migration Planning for M&A, Divestiture				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]

Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal				119,976.00
Total Estimated Fees (excluded taxes)				**119,976.00**
Modern Workplace - Program Governance-2021-22				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Client Interface – Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]
Client Interface – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal				173,168.00
Total Estimated Fees (excluded taxes)				**173,168.00**
Office 365 Migration for M&A, Divestiture - UB-2021-22				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Follow	[redacted]	[redacted]	[redacted]	[redacted]
Client Interface - Follow	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Follow	[redacted]	[redacted]	[redacted]	[redacted]

Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Follow	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]

Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Exchange Migration Between Tenants - Mailbox migration factory	[redacted]	[redacted]	[redacted]	[redacted]
OneDrive Migration Between Tenants - Azure Subscription	[redacted]	[redacted]	[redacted]	[redacted]
Procured Material	[redacted]	[redacted]	[redacted]	[redacted]
Teams Migration - Azure Subscription	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal				580,892.50
Total Estimated Fees (excluded taxes)				**580,892.50**
Modern Workplace Adoption and Change Management Assessment-2021-22				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Client Interface – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]

Subtotal				74,184.00
Total Estimated Fees (excluded taxes)				**74,184.00**
Endpoint and Application Management - UB				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Application Packaging	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal				177,796.10
Total Estimated Fees (excluded taxes)				**177,796.10**
Tier 1 - 1 to 10 Directories				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Tier 1 - Cloud Synchronization Estimated Months	[redacted]	[redacted]	[redacted]	[redacted]

Tier 1 - Connected Directories to Synchronize	[redacted]	[redacted]	[redacted]	[redacted]
Tier 1 - On-Prem Synchronization Estimated Months	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal				97,999.80
Total Estimated Fees (excluded taxes)				**97,999.80**
Azure Workloads for WVD-2021-22				
Role/Service	**Rate**	**Quantity**	**Subtotal**	**Total GBP**
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Client Interface – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation - Initiate or influence	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Solution development and implementation – Ensure or advise	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal				168,000.00
Total Estimated Fees (excluded taxes)				**168,000.00**

Customer will pay the fixed fee price as set forth below plus any expenses (estimates outlined in Services Fees table below). The fees do not include fees for Products. Microsoft will invoice Customer the fixed fee on a milestone basis according to the estimated milestone schedule listed in Billing Schedule table below. Microsoft will invoice Customer monthly for expenses. Unless otherwise specified in the invoice, Customer will pay Microsoft within 30 calendar days of the date of Microsoft invoice.

Service Fees		
Packages	**Estimated Date**	**Total GBP**
SharePoint Migration Service	[redacted]	[redacted]
Subtotal		[redacted]
Total Fees (excluding taxes)		**122,399.00**

Billing Schedule	**Estimated Date**	**Fee GBP**
Month 1 SharePoint Migration Service	[redacted]	[redacted]
Month 2 SharePoint Migration Service	[redacted]	[redacted]
Total Fees (excluding taxes)		**122,399.00**

Part B: Terms and Conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection)
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation

- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'.

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'.

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract.

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.1.6 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5 Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party.

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer’s own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier’s delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer’s failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there’s an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn’t possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer’s volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 During this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000.

9.2.2 the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit.

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the CallOff Contract, and for 6 years after the End or Expiry Date.

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date.

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance.

9.4.2 receipts for the insurance premium.

9.4.3 evidence of payment of the latest premiums due.

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers.

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances.

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance.

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly.

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royaltyfree licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.5.1 rights granted to the Buyer under this Call-Off Contract.

11.5.2 Supplier's performance of the Services.

11.5.3 use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.6.1 modify the relevant part of the Services without reducing its functionality or performance.

11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer.

11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer.

11.7 Clause 11.5 will not apply if the IPR Claim is from:

11.7.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract.

11.7.2 other material provided by the Buyer necessary for the Services.

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data.

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body.

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes.

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request.

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions.

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer).

12.2.4 providing the Buyer with any information requested by the Data Subject.

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier’s and Buyer’s security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy: https://www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.cpni.gov.uk/protectionsensitive-information-and-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technology-code-ofpractice/technology-code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-securityprinciples

13.6.6 buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer

immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:

https://www.gov.uk/government/publications/technology-code-of-practice/technology-codeof-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security
Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided.

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control.

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5.

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee.

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided.

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses.

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The

Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied.

18.4.2 any fraud.

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so.

18.5.2 an Insolvency Event of the other Party happens.

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business.

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration.

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry.

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses.

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry) • 24 (Liability); incorporated Framework Agreement clauses:
- 4.2 to 4.7 (Liability).
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it.

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer.

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer.

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law.

19.5.5 work with the Buyer on any ongoing work.

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date.

19.6 Each Party will return all of the other Party’s Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending.
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message.

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this CallOff Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer.

21.6.2 there will be no adverse impact on service continuity.

21.6.3 there is no vendor lock-in to the Supplier's Service at exit.

21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice.

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier.

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer.

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier.

21.8.4 the testing and assurance strategy for exported Buyer Data.

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations.

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition.

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier’s possession, power or control.

22.1.2 other information reasonably requested by the Buyer.

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order

Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form.

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form.

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

25.1 If either Party uses the other Party’s premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer’s premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises.

25.5.2 comply with Buyer requirements for the conduct of personnel.

25.5.3 comply with any health and safety measures implemented by the Buyer.

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury.

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn’t Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform

29.2.2 age

29.2.3 start date

29.2.4 place of work

29.2.5 notice period

29.2.6 redundancy payment entitlement

29.2.7 salary, benefits and pension entitlements

29.2.8 employment status

29.2.9 identity of employer

29.2.10 working arrangements

29.2.11 outstanding liabilities

29.2.12 sickness absence

29.2.13 copies of all relevant employment contracts and related documents

29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause.

29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer.

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	**Meaning**
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn’t available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.

Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.

Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/oractual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) the GDPR, the LED and any applicable national implementing laws as amended from time to time. ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy. all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term). • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract. Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk)
DPA 2018	Data Protection Act 2018.

Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employmentstatus-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.

G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand a Schedule A1 moratorium

Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information. • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction. all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier’s or CCS’s possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.

LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice’s Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.

Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's background IPRs.

Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's highperformance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.

Service data	Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the GCloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier’s servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier’s Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDRP information

The Microsoft Professional Services Data Protection Addendum, as incorporated into this Call-Off Contract, shall apply.

UK Health
Security
Agency

Statement of Work

Merger, Acquisition, Divestiture Migration for Modern Workand WVD

Date: 08/05/2021 | Version: 4.0

Prepared for
UK Health Security Agency

Prepared by
Gabriel Antohi
Microsoft Modern Work Architect

Microsoft

Table of Contents

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]

Introduction

[redacted]

[redacted]

[redacted]	[redacted]
	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

1. The Microsoft Services Programme to deliver the Requirements

1.1. Programme Objectives

[redacted]

[redacted]

ID	Component Name
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
ID	Component Name

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

1.2. Areas in Scope

1.2.1. General Project Scope

[redacted]

Component (ID)	Description	Assumptions
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions
	[redacted]	
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions

	[redacted]	[redacted]

Component (ID)	Description	Assumptions
		[redacted]
[redacted]	[redacted]	[redacted] Office 365 desired state configuration module (DSC) [redacted] [redacted] GitHub

[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions

	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions
	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions

	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Component (ID)	Description	Assumptions
	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Component (ID)	**Description**	**Assumptions**

[redacted]	[redacted]	[redacted]

1.2.2. Software Products and Technologies

[redacted]

Component ID	Product and Technology Item	Version	Ready by
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Component ID	Product and Technology Item	Version	Ready by
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]

1.2.3. Environments

[redacted]

Component ID	Environment	Location	Responsibility	Ready by
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Component ID	**Environment**	**Location**	**Responsibility**	**Ready by**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1.2.4. Testing and Defect Remediation

1.2.4.1. Testing

[redacted]

Component ID	Test Type	Description	Responsibility		
	(Environment)		Has Responsibility for Testing?	Provides Data or Test Cases	Provides Guidance and Support
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Component ID	Test Type	Description	Responsibility		
	(Environment)		Has Responsibility for Testing?	Provides Data or Test Cases	Provides Guidance and Support
		[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Component ID	Test Type	Description	Responsibility		
	(Environment)		Has Responsibility for Testing?	Provides Data or Test Cases	Provides Guidance and Support
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

1.2.4.2. Defect remediation

[redacted]

[redacted]

[redacted]

Priority	Description	Remediation in Scope?
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

1.3. Areas Out of Scope

[redacted]

Component ID	Area	Description

[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

Component ID	Area	Description
	[redacted]	[redacted]

	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]

Component ID	Area	Description
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

	[redacted]	[redacted]

Component ID	Area	Description
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

Component ID	Area	Description
		[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

Component ID	Area	Description

		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Component ID	Area	Description
		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Component ID	Area	Description
		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

Component ID	Area	Description
		[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

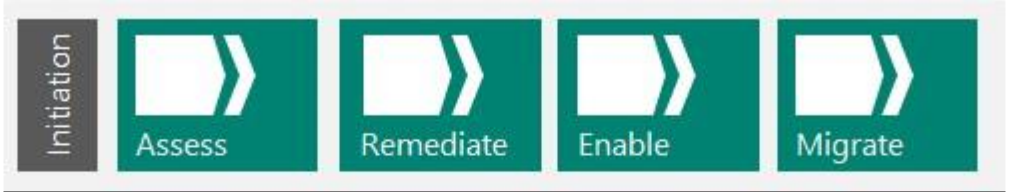
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

2. Project Approach and Timeline

[redacted]

2.1. Approach - All Components Except for WVD-01

[redacted]



[redacted]

[redacted]

2.1.1. Engagement Initiation

[redacted]

Category	ID	Description

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

2.1.2. General Project Activities

[redacted]

Category	Description

[redacted]	[redacted] Project Components and Work Products [redacted]

Category	Description

	[redacted] [redacted] [redacted] Project Components and Work Products [redacted]
[redacted]	[redacted] [redacted] Timeline [redacted] [redacted] [redacted] General project scope [redacted] [redacted] [redacted]

Category	Description
	[redacted]
[redacted]	[redacted]

2.1.2.1. General Project Components

[redacted]

[redacted] Project Components and Work Products.

Name	Description	Phase	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
Name	**Description**	**Phase**	**Responsibility**
	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

2.1.3. Project Components and Work Products

[redacted]

2.1.3.1. Microsoft 365 Migration Planning for Merger, Acquisition, or Divestiture (MAD-01)

Category	Description

[redacted]	[redacted]
Category	**Description**
	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.2. Azure Active Directory Integration for Forest Restructuring (AAD-03)

Category	**Description**

[redacted]	[redacted]

Category	Description
	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.3. Exchange Migration Between Tenants (EMT-01)

Category	Description

[redacted]	[redacted]

Category	Description
	[redacted]
[redacted]	[redacted]

Category	Description
	[redacted]
[redacted]	[redacted]

2.1.3.4. Office 365 Configuration Migration Between Tenants (OCM-01)

Category	Description
[redacted]	[redacted]

[redacted]	[redacted]
Category	**Description**
	[redacted]
[redacted]	[redacted]

2.1.3.5. OneDrive Migration Between Tenants (ODT-01)

Category	**Description**

[redacted]	[redacted]

Category	Description

	[redacted]
[redacted]	[redacted]

Category	Description
	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.6. Microsoft Teams Migration Between Tenants (TMT-01)

Category	Description

[redacted]	[redacted]

Category	Description
	[redacted]

[redacted]	[redacted]

Category	Description
	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]

[redacted]

[redacted]

Name	Description	Phase	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]

2.1.3.7. SharePoint Online Content Migration (SPO-01)

Category	Description

[redacted]	[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

Category	Description
	[redacted]

[redacted]	[redacted]

Category	Description

	[redacted]

Category	Description

[redacted]	[redacted]

Category	Description
	[redacted]

[redacted]	[redacted]

2.1.3.8. Active Directory Synchronisation Services (Component ADS-01)

[redacted]

Category	Description
[redacted]	[redacted]

[redacted]	[redacted]
Category	**Description**
	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.9. Client Migration Between Tenants (CMT-01)

Category	**Description**

[redacted]	[redacted]

Category	Description
	[redacted] 1.2.5. Testing and defect remediation [redacted]

[redacted]	[redacted]
Category	**Description**
[redacted]	[redacted]

[redacted]	[redacted]

[redacted]

Name	Description	Phase	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]

2.1.3.10. Windows Autopilot Enablement (WDAP-02)

Category	Description

[redacted]	[redacted]
[redacted]	[redacted]

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.11. Intune Application Delivery (APP-02)

Category	Description

[redacted]	[redacted]

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.12. Intune Application Protection (APP-03)

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.13. Application Packaging (PAC-01)

Category	Description
[redacted]	
[redacted]	[redacted]

	[redacted]

Category	Description
[redacted]	[redacted]

	- [redacted] - [redacted] - [redacted] [redacted] [redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Category	**Description**
[redacted]	

[redacted]

Name	**Description**	**Phase**	**Responsibility**

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

2.1.3.14. Intune Device Management (MDM-01)

Category	Description
[redacted]	[redacted]

Category	Description

	[redacted]
[redacted]	[redacted]

	[redacted]

Category	Description

	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.15. Intune Device Management Certificate Deployment (MDM-02)

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.16. Windows Security Foundations (SEC-01)

Category	Description

[redacted]	[redacted]

Category	Description
	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.17. Additional Support for configuring PHECloud as alternate identify provider (AAD-01)

Category	Description
[redacted]	[redacted]
Category	**Description**
	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

2.1.3.18. Modern Workplace Adoption and Change Management Assessment (ACM-01)

Category	Description

[redacted]

[redacted]

Category	Description
	[redacted] [redacted] [redacted] [redacted] [redacted]

Category	Description
	[redacted]
[redacted]	
[redacted] [redacted]	[redacted]
[redacted]	
	[redacted]

Category	Description
	[redacted]

[redacted]

[redacted]

[redacted]

Name	Description	Phase	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]

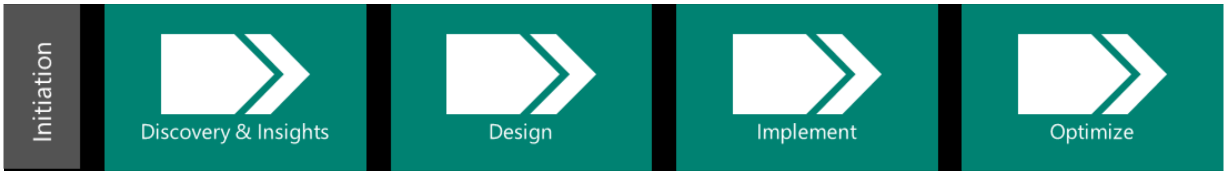
Category	Description

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Name	Description	Phase	Responsibility
	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]

2.2. Approach for WVD-001

[redacted]



2.2.1. Engagement Initiation

[redacted]

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]

2.2.2. Discovery and Insights

[redacted]

Discovery & Insights Design Implement Optimize

Category	Description

[redacted]	[redacted]

Discovery & Insights Design Implement Optimize

Category	Description
	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

Name	Description	Responsibility
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

2.2.3. Design

[redacted]

Discovery & Insights Design Implement Optimize

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

Name	Description	Acceptance Required?	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]

2.2.4. Implement

[redacted]

Discovery & Insights Design Implement Optimize

Category	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

Name	Description	Acceptance Required?	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

2.2.5. Optimise

[redacted]

Discovery & Insights Design Implement Optimize	
Category	**Description**
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]

Discovery & Insights Design Implement Optimize

Category	Description
	[redacted]

[redacted]

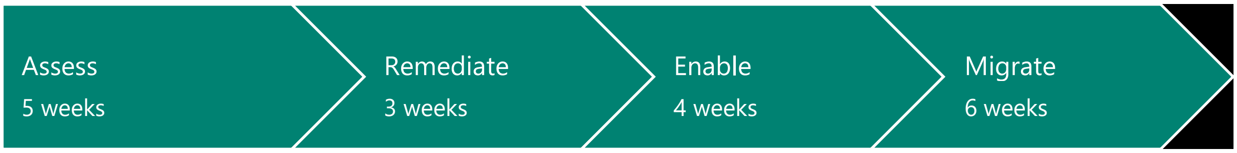
Name	Description	Acceptance Required?	Responsibility
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

2.3. Timelines

2.3.1. Timeline for all components except WVD-01

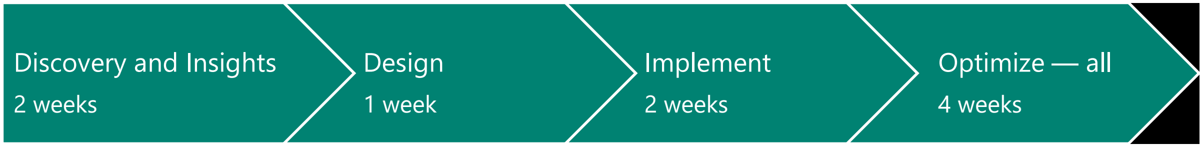
[redacted]

[redacted]



2.3.2. Timeline for WVD-01

[redacted]



2.4. Project Governance

[redacted]

2.4.1. Project Communication

[redacted]

- [redacted]
- [redacted]
- [redacted]

2.4.2. Risk and Issue Management

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

2.4.3. Change Management Process

[redacted]

[redacted]

[redacted]

[redacted]

2.4.4. Executive Steering Committee

[redacted]

[redacted]

Role	Organisation
[redacted]	[redacted]
[redacted]	[redacted]

2.4.5. Escalation Path

[redacted]

[redacted]

2.5. Project Completion

[redacted]

[redacted]

[redacted]

ID	Component Name	Fee Arrangement
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	

[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	

ID	Component Name	Fee Arrangement
[redacted]	[redacted]	
[redacted]	[redacted]	

3. Project Organisation

3.1. Project Roles and Responsibilities

[redacted]

3.1.1. UKHSA

Role	Component ID(s)	Responsibilities
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Role	Component ID(s)	Responsibilities
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Role	Component ID(s)	Responsibilities
		[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Role	Component ID(s)	Responsibilities

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Role	Component ID(s)	Responsibilities
		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
Role	**Component ID(s)**	**Responsibilities**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

3.1.2. Microsoft

Role	Component ID(s)	Responsibilities
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Role	Component ID(s)	Responsibilities
		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Role	Component ID(s)	Responsibilities
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4. UKHSA Responsibilities and Project Assumptions

4.1. UKHSA Responsibilities

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

4.2. Project Assumptions

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5. Appendix: Service Descriptions

5.1. Appendix: Active Directory Synchronisation Service (ADSS)

[redacted]

[redacted]

Object type	Windows Active Directory Domain Sync	Azure Active Directory Tenant Sync
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

5.1.1. Acceptance Process

[redacted]

- [redacted]
- [redacted]

5.1.2. Service Acceptance

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

5.1.3. Project Completion

[redacted]

5.1.4. Components and Service Definitions

[redacted]

Component	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Component	Description

	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

5.2. SharePoint Online Content Migration Units

[redacted]

Migration unit	Definition

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Microsoft Professional Services

Data Protection Addendum

November 2020

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the Agreement. The following defined terms are used in this DPA:

"Agreement" means as applicable the Description of Services and any Exhibits, Statements of Work, Enterprise Services Work Order(s), Microsoft Business Support Services Work Order(s), and the applicable Microsoft master agreement, such as the Microsoft Business and Services Agreement.

"Data Protection Requirements" means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"DPA Terms" or "DPA" means the terms in this DPA.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"GDPR Terms" means the terms in Attachment 2, under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"Online Service" means a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms. It does not include software and services provided under separate license terms (such as via gallery, marketplace, console, or dialog). The Product Terms is located at http://go.microsoft.com/?linkid=9839207.

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Professional Services" means the following services provided under an Enterprise Services Work Order: (a) professional planning, advice, guidance, data migration, deployment and solution/software development services provided by Microsoft Consulting Services ("Consulting Services"); and (b) Microsoft Unified Support or Premier Support Services as described in the Services Consulting and Support Description or the Description of Services, respectively, which consist of professional technical software support services provided by Microsoft that help customers identify and resolve issues in their information technology environment ("Support Services"). Additionally, Professional Services includes (c) services provided under a Microsoft Business Support Services Work Order. The Professional Services do not include the Online Services.

"Professional Services Data" means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

"Standard Contractual Clauses" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The Standard Contractual Clauses are in Attachment 1.

"Subprocessor" means other processors used by Microsoft to process Professional Services Data, including any subcontractor that processes Professional Services Data.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses.

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its provision of the Professional Services including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Professional Services Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of the Professional Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Professional Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Professional Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of a Professional Service.

Acceptable Use Policy

Neither Customer nor their representatives may use Professional Services or the Services Deliverables:

 in a way prohibited by law, regulation, governmental order or decree;

- to violate the rights of others;
- to try to gain unauthorized access to or disrupt any service, device, data, account or network;
- to spam or distribute malware;
- in a way that could harm Microsoft's IT systems or impair anyone else's use of them;
- in any application or situation where use of the Professional Services (or Services Deliverables) could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage*, except in accordance with the High Risk Use section below*; or to assist or encourage anyone to do any of the above.

High Risk Use

WARNING: Modern technologies may be used in new and innovative ways, and Customer must consider whether its specific use of these technologies is safe. The Services and Services Deliverables will not be designed or intended to support any use in which a service interruption, defect, error, or other failure of a Services Deliverable could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "High Risk Use"). Accordingly, Customer must implement every Services Deliverable such that, in the event of any interruption, defect, error, or other failure of each Service Deliverable, the safety of people, property, and the environment are not reduced below a level that is reasonable, appropriate, and legal, whether in general or for a specific industry. Customer's High Risk Use of the Services and Services Deliverables is at its own risk. Customer agrees to defend, indemnify and hold Microsoft harmless from and against all damages, costs and attorneys' fees in connection with any claims arising from a High Risk Use associated with the Services and Services Deliverables, including any claims based in strict liability or that Microsoft was negligent in designing or providing the Service(s) and Services Deliverables to Customer. The foregoing indemnification obligation is in addition to any defense obligation set forth in Customer's Agreement and is not subject to any limitation of, or exclusion from, liability contained in such agreements.

Online Services

For applicable Online Services engagements: To assist in evaluating Professional Services delivery, Customer agrees to provide Microsoft access to usage metrics within their Online Services. No Personal Data from the Online Service is included within the metrics.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Processing; Ownership;
- Disclosure of Professional Services Data
- Processing of Personal Data; GDPR
- Data Security

Scope

The terms in this DPA apply to all Professional Services except as described within this section.

Previews

Previews may employ lesser or different privacy and security measures than those typically present in the Professional Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. Previews meet only the terms of the sections "Processing of Personal Data; GDPR", the first paragraph of "Security Practices and Policies" under "Data Security", the first two paragraphs of "Notice and Controls on Use of Subprocessors" and the GDPR Terms.

Previews means preview, beta, offers for optional evaluation, or other pre-release or limited release services or features, including any designated or labeled as such.

Escalation Support

The Microsoft Online Services Data Protection Addendum Attachment 1, available at http://aka.ms/mpstomosdpa, includes the privacy and security terms for escalation support, meaning support requests escalated to Online Services engineering or operations for resolution, including any Personal Data therein ("Escalation Support"). Therefore, the terms in this DPA do not apply to the provision of Escalation Support.

Nature of Processing; Ownership

Microsoft will use and otherwise process Professional Services Data only to provide Customer the Professional Services in accordance with Customer's documented instructions. As between the parties, Customer retains all right, title and interest in and to Professional Services Data. Microsoft acquires no rights in Professional Services Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in Products or Online Services Microsoft licenses to Customer.

Processing to Provide Customer the Professional Services

For purposes of this DPA, "to provide" Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services. For the removal of doubt, providing technical support will include making improvements to the underlying Microsoft products and services subscribed to or utilized by Customer based on issues identified during delivery of Professional Services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified during delivery of Professional Services); and
- Ongoing improvement of Professional Services subscribed to or utilized by Customer (maintaining the Professional Services, making improvements to the reliability, efficacy, quality, and security of the Professional Services and fixing software defects).

When providing Professional Services, Microsoft will not use or otherwise process Professional Services Data for (a) user profiling, or (b) advertising or similar commercial purposes or (c) market research aimed at creating new functionalities, services, or products or any other purpose,, unless such use or processing is in accordance with Customer's documented instructions.

Disclosure of Processed Data

Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Professional Services Data; (b) Personal Data included in Professional Services Data; and (c) any other data processed by Microsoft in connection with the Professional Service that is Customer's confidential information under the Agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the Agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts

Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data included in Professional Services Data and provided to Microsoft by, or on behalf of, Customer through an engagement with Microsoft to obtain Professional Services is also Professional Services Data. Pseudonymized identifiers may also be generated through Professional Services IT systems and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 2 govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its Agreement (including this DPA Terms and any applicable updates), along with the Professional Services documentation and Customer's use of Professional Services,) are Customer's complete documented instructions to Microsoft for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Professional Services pursuant to Customer's Agreement (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).
- **Categories of Data.** The types of Personal Data processed by Microsoft when providing Professional Services include: (i) Personal Data that Customer elects to include in Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR. The types of Personal Data that Customer elects to include in Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix 1 to Attachment 1 – The Standard Contractual Clauses (Processors) of the DPA.
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix 1 to Attachment 1 – The Standard Contractual Clauses (Processors) of the DPA.

Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Professional Services and Microsoft's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Professional Services for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to

Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality provided to Customer for that purpose. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Professional Services Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with descriptions of the security controls in place for the Professional Service and other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Professional Services also implements and maintains the security measures set forth in Appendix A for the protection of Professional Services Data..

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or the standards or frameworks in the table in Attachment 1 to the OST (or successor location in the Use Rights), unless it is no longer used in the industry and it is replaced with a successor (if any).

Data Encryption

Professional Services Data (including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Data Access

Microsoft employs least privilege access mechanisms to control access to Professional Services Data (including any Personal Data therein). Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A – Notices. Role-based access controls are employed to ensure that access to Professional Services Data required for service operations is for an appropriate purpose and approved with management oversight.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Professional Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls.

Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Professional Services Data as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third-party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to nondisclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer’s audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer’s additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Professional Services Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft’s other customers or to Microsoft systems or facilities not involved in the Professional Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer’s audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material noncompliance.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses.

Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority’s or data subject’s rights under the Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended thirdparty beneficiary of this section.

Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Professional Services Data while processed by Microsoft (each a “Security Incident”), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer’s business contacts for the Professional Services by any means Microsoft selects, including via email. It is Customer’s sole responsibility to ensure Customer’s business contacts maintain accurate contact information.

Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any thirdparty notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer’s obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft’s notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Professional Services.

Data Transfers

Professional Services Data that Microsoft processes on Customer’s behalf may be transferred to, and stored and processed in the United States or any other country in which Microsoft or its Subprocessors operate. Customer appoints Microsoft to perform any such transfer of Professional Services Data to any such country and to store and process Professional Services Data in order to provide the Professional Services.

All transfers of Professional Services Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Professional Services shall be governed by the Standard Contractual Clauses in Attachment 2.

Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Professional Services Data Deletion

At all times during the term of Customer's Professional Services engagement, Customer will have the ability to access, extract and delete Professional Services Data.

Microsoft will delete all copies of Professional Services Data after the business purposes for which the Professional Services Data was collected or transferred have been fulfilled, or earlier upon Customer's written request.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Professional Services Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Professional Services Data in accordance with laws applicable to Microsoft as a provider of professional IT services, Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Professional Services Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Professional Services Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Professional Services Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

For Support Services, a list of Microsoft's current Subprocessors is available at: https://aka.ms/servicesapprovedsuppliers. From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 30-days in advance of providing that Subprocessor with access to Professional Services Data.

For Consulting Services, notice of Subprocessors that will be used during performance of work is available upon request at https://aka.ms/consultingapprovedsuppliers. Customer may also request to be notified of updates to the Subprocessors that will be used during performance of work. For customers that have requested to be notified of updates to the Subprocessors that will be used during performance of work, Microsoft will not grant access to Professional Services Data until written approval is provided or 30-days from notification.

If Customer does not approve of a new Subprocessor, then Customer may terminate the applicable Statements of Service, such as an Enterprise Services Work Order, for the affected Professional Services without termination fee by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. After termination, Microsoft will remove payment obligations for any applicable unpaid work for the terminated Professional Services from subsequent invoices to Customer.

California Consumer Privacy Act (CCPA) Terms

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Professional Services Data on behalf of Customer and not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA or any other agreement between Microsoft and Customer.

Biometric Data

If Customer uses a Professional Service to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations Ltd.
Attn: Data Protection
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

Appendix A – Security Measures

Microsoft has implemented and will maintain for Professional Services Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms) are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership.** Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities.** Microsoft personnel with access to Professional Services Data are subject to confidentiality obligations. **Risk Management Program.** Microsoft performed a risk assessment before processing Professional Services Data. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory.** Microsoft maintains an inventory of all media on which Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling.** - Microsoft classifies Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Professional Services Data and has procedures for disposing of printed materials that contain Professional Services Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Professional Services Data on portable devices, remotely accessing Professional Services Data, or processing Professional Services Data outside Microsoft's facilities.
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities.** Microsoft limits access to facilities where information systems that process Professional Services Data are located to identified authorized individuals. **Physical Access to Components.** Microsoft maintains records of the incoming and outgoing media containing Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Professional Services Data they contain. **Protection from Disruptions.** Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal.** Microsoft uses industry standard processes to delete Professional Services Data when it is no longer needed.

Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Professional Services Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Professional Services Data has been updated during that period), Microsoft maintains multiple copies of Professional Services Data from which Professional Services Data can be recovered. - Microsoft stores copies of Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Professional Services Data is located. - Microsoft has specific procedures in place governing access to copies of Professional Services Data. - Microsoft reviews data recovery procedures at least annually. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and, where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Professional Services Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Microsoft encrypts, or enables Customer to encrypt, Professional Services Data that is transmitted over public networks.
Domain	Practices
	- Microsoft restricts access to Professional Services Data in media leaving its facilities. **Event Logging** - Microsoft logs, or enables Customer to log, access and use of information systems containing Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.

Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Professional Services Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Professional Services Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Professional Services Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Professional Services Data when needed. - Microsoft restricts access to Professional Services Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Professional Services Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - Microsoft tracks, or enables Customer to track, disclosures of Professional Services Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Professional Services Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

Attachment 1 – The Standard Contractual Clauses (Processors) for Professional Services

Execution of a statement of services by Customer includes execution of this Attachment 1, which is countersigned by Microsoft Corporation.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

All references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire

legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses for Professional Services

Data exporter: Customer is the data exporter. The data exporter is procuring professional IT support and consulting services as described in the applicable Enterprise Services Work Order or Microsoft Business Support Services Work Order.

Data importer: The data importer is MICROSOFT CORPORATION, a global producer of software and services.

Data subjects: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Microsoft acknowledges that, depending on Customer's use of the Professional Service, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter); • Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of data: The personal data transferred that is included in e-mail, documents and other data in an electronic form in the context of the Professional Services. Microsoft acknowledges that, depending on Customer's use of the Professional Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;

□ Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or □ Any other personal data identified in Article 4 of the GDPR.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

a. **Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under the applicable volume licensing agreement between data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of the Professional Services.

b. **Scope and Purpose of Data Processing.** The scope and purpose of processing personal data is described in the "Processing of Personal Data; GDPR" section of this the DPA. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the "Security Practices and Policies" section of the DPA.

c. **Professional Services Data Access.** For the term designated under the Agreement, the data importer will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Professional Services Data, or (2) make such corrections, deletions, or blockages on its behalf.

d. **Data Exporter's Instructions.** For Professional Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

e. **Professional Services Data Deletion.** Upon expiration or termination of data exporter's use of Professional Services, data importer will delete Professional Services in accordance with the DPA Terms applicable to the agreement.

Subcontractors: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf. Any such subcontractors will be permitted to obtain Professional Services Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Professional Services Data for any other purpose.

Appendix 2 to the Standard Contractual Clauses for Professional Services

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Personnel**. Data importer's personnel will not process Professional Services Data without authorization. Personnel are obligated to maintain the confidentiality of any such Professional Services Data and this obligation continues even after their engagement ends.

2. **Data Privacy Contact**. The data privacy officer of the data importer can be reached at the following address: Microsoft Corporation
Attn: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052 USA

3. **Technical and Organization Measures**. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Professional Services Data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. The technical and organizational measures, internal controls, and information security routines set forth in Security Practices and Policies section of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signing the Standard Contractual Clauses for Professional Services, Appendix 1 and Appendix 2 on behalf of the data importer:

Attachment 2 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the DPA that is otherwise applicable to any given engagement or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Customer Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer.

These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Microsoft Professional Services Data Protection Addendum or other agreement between Microsoft and Customer.

These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))

2. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's Agreement, including these GDPR Terms. In particular, Microsoft shall:

(a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) take all measures required pursuant to Article 32 of the GDPR;

(d) respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;

(e) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

(f) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;

(g) at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;

(h) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

3. Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under

Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations,
Microsoft shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

4. 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, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
(Article 32(2))

6. Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

7. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

Microsoft & PHE G Cloud 12 Contract

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

✓ [redacted]

[redacted]