.

G-Cloud 13 Call-Off Contract between

Competition and Markets Authority and

Unit4 Business Software Limited

.

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.

Platform service ID number	Lot 2 - Service ID Cloud Software 509645900118293
Call-Off Contract reference	Buyer Ref: PROC 861-2024 Supplier Ref: UKI/2024/U4ERP/U4-135019
Call-Off Contract title	CMA ERP Solution - Unit4 [Enterprise Resource Planning Solutions]
Call-Off Contract description	Contract for the delivery of Unit4 solutions, including Unit4 SaaS
Start date	1 June 2024
Expiry date	31 May 2025 (subject to optional extension period mentioned below)
Call-Off Contract value	£291,743.99 + VAT
Charging method	By invoice
Purchase order number	To Follow

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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 Services 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	**Buyer Name**:	Competition & Markets Authority
	Buyer Phone Number:	020 3738 6000
	Buyer Address:	The Cabot, 25 Cabot Square, London, E14 4QZ
	Company registration number:	Not applicable
To the Supplier	**Supplier Name**:	Unit4 Business Software Limited
	Supplier Phone Number:	01275 377 205
	Supplier's Address:	C/O DAC Beachcroft LLP, Portwall Place, Portwall Lane, Bristol, BS1 9HS
	Company registration number:	01737985
Together the 'Parties'		

Principal contact details

For the Buyer:

Title: [redacted]
Name: [redacted]
Email: [redacted]
Phone: [redacted]

For the Supplier:

Title: [redacted]
Name: [redacted]
Email: [redacted]
Phone: [redacted]

.

Call-Off Contract term

Start date	This Call-Off Contract Starts on **1 June 2024** and is valid for **12 months**.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **30** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a minimum of 1 year from the date of written notice before the end of the initial term or the relevant extension period for Ending without cause (as per clause 18.1). The Buyer and Supplier agree this period is necessary and reasonable given the nature of the services provided to the Buyer.
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the 30 days' written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-contr ols-check-if-you-need-approval-to-spend-money-on-a-service

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 2: Cloud software
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: ● Lot 2: Cloud software

.

Additional Services	None
Location	System provision will be provided from Unit4's infrastructure provider's data centres as specified in paragraph 6 of Part A of Schedule 7 of this Call-Off Contract. Unit4 support services will primarily be delivered from Unit4's support service centres in the United Kingdom, Ireland, Portugal and Poland, but can include other EU countries. Where required, support may be provided from any of the countries listed in paragraph 6 of Part A of Schedule 7 of this Call-Off Contract.
Quality Standards	The quality standards required for this Call-Off Contract are as described in the Unit4 Cloud Service Description Unit4 ERP 7 of the Unit4 Lot 2 Service Descriptions which is available at: Unit4 Cloud Service Description - Unit4 ERP 7 v.1.9 (EN) (digitalmarketplace.service.gov.uk)
Technical Standards:	The technical standards used as a requirement for this Call- Off Contract are as described in the Unit4 Cloud Service Description Unit4 ERP 7 of the Unit4 Lot 2 Service Descriptions which is available at: Unit4 Cloud Service Description - Unit4 ERP 7 v.1.9 (EN) (digitalmarketplace.service.gov.uk)
Service level agreement:	The Supplier's cloud service levels are as described in the Unit4 SaaS – Service Level Agreement of the Supplier Terms and the Supplier's support levels are described in the Unit4 Support Terms – Standard Support of the Supplier Terms, each available at: Unit4 General Terms of Business (Dynamic) v.2.1 April 2021 (EN - UKI) (digitalmarketplace.service.gov.uk)
Onboarding	As the Buyer is an existing customer of the Supplier and has previously completed onboarding this is not applicable to this Call-Off Contract.
Offboarding	The offboarding plan for this Call-Off Contract is as described in clause 8.4 [Where SaaS] of the Unit4 General Terms of Business of the Supplier Terms, available at: Unit4 General Terms of Business (Dynamic) v.2.1 April 2021 (EN - UKI) (digitalmarketplace.service.gov.uk).]

.

Collaboration agreement	Not Required.
Limit on Parties' liability	Defaults by either Party resulting in direct loss to the Property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed the lower of (a) 100% of the Charges payable by the Buyer to the Supplier in the 12-month period preceding such Default or (b) £1,000,000, per year. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed £1,000,000 or 100% of the Charges payable by the Buyer to the Supplier in the 12-month period preceding such Default (whichever is the lower). The annual total liability of the Supplier for all other Defaults will not exceed £500,000 or 100% of the Charges payable by the Buyer to the Supplier in the 12-month period preceding such Default (whichever is the lower).
Insurance	The Supplier 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, Sub-Contractor 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 required by Law; and • employers' liability insurance with a minimum limit of £5,000,000 or such higher minimum limit required by Law.
Buyer's responsibilities	Buyer shall comply with all the Buyer's responsibilities and obligations set out in the Supplier Terms.
Buyer's equipment	Not applicable to this Call-Off Contract.

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners: *There are none*.

.

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: ***Unit4 SaaS fees:*** Invoice will be raised following execution of this Call-Off Contract, and the invoice will be due for payment within 30 days. Subsequent invoices issued annually in advance.
Invoice details	The Supplier will issue electronic invoices in accordance with the Payment Profile above. The Buyer will pay the Supplier within 30 calendar days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Electronic version of the invoices shall be sent to Invoices@cma.gov.uk and addressed to: Accounts Payable.
Invoice information required	All invoices must include: • Items, unit costs and period being charged. • Valid CMA PO number
Invoice frequency	Invoice will be sent to the Buyer as per the Payment Profile above.
Call-Off Contract value	The total value of this Call-Off Contract is **£291,743.99 + VAT**
Call-Off Contract charges	The breakdown of the Charges is set out in Schedule 2.

.

Additional Buyer terms

Performance of the Service	The Service will be delivered in accordance with the Unit4 Cloud Service Description Unit4 ERP 7 of the Unit4 Lot 2 Service Descriptions which is available which is available at: Unit4 Cloud Service Description - Unit4 ERP 7 v.1.9 (EN) (digitalmarketplace.service.gov.uk).
Guarantee	None Required.
Warranties, representations	None Required.
Supplemental requirements in addition to the Call-Off terms	In accordance with Call-Off Contract clauses, the Supplier will comply with the Supplier Terms available at: Unit4 General Terms of Business (Dynamic) v.2.1 April 2021 (EN - UKI) (digitalmarketplace.service.gov.uk) 

	
Alternative clauses	Not applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	[redacted]

.

Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1 is being used and the wording of Annex 2 has been deleted from this Call-Off Contract.
Intellectual Property	The Supplier (or, where applicable, the Third Party Provider) owns all IPRs in and to the Unit4 Products, Unit4 Services, Unit4 Documentation and all other Unit4 IPRs. Subject to the limited rights expressly granted in this Call-Off Contract, Unit4 reserves all rights, title and interest in and to the Unit4 Product, all goodwill associated with the same and all related IPRs. Terms used in this paragraph have the meanings given to them in the Supplier Terms available on the Public Procurement Gateway. Clause 11.4 of Part B: Terms and Conditions of this Call-Off Contract is deleted and replaced with clause 5.2 [Where SaaS] of the Unit4 General Terms of Business of the Supplier Terms. The Parties agree that no Project Specific IPRs will be created or arise out of the performance by the Supplier (or by a third party on behalf of the Supplier) of its obligations under this Call-Off Contract.
Social Value	None Required.

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 RM1557.13

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

Signed	**Supplier:** **UNIT4 BUSINESS SOFTWARE LIMITED**	**Buyer:** **COMPETITION & MARKETS AUTHORITY**
Name	[redacted]	
Title		
Signature		
Date		

.

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

G-Cloud 13 Customer Benefit Record

.

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 36 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 1 period of up to 12 months.

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 set the Term at more than 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:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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’ or to ‘CCS and/or the Buyer’ 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 7 (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

4.2 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 14digit 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 their 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 Call-Off 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 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 incorporated Framework Agreement clause 34. 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 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;

(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer 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:

11.6.1 rights granted to the Buyer under this Call-Off Contract

.

11.6.2 Supplier’s performance of the Services

11.6.3 use by the Buyer of the Services

11.7 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:

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

11.7.2 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

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

11.8 Clause 11.6 will not apply if the IPR Claim is from:

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, 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-securityclassifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-managementapproach and Protection of Sensitive Information and Assets: https://www.cpni.gov.uk/protection-sensitive-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/technologycode-of-practice/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-security-principles

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-code-of-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. 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 are reasonable compensation and cover 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); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
- 24 (Conflicts of interest and ethical walls), 35 (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 Call-Off 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 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 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 take the Term beyond 36 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 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 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

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

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.

29.3 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.

29.4 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.

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

29.5.1 its failure to comply with the provisions of this clause

29.5.2 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

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

.

29.7 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, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

.

Schedule 1: Services

1. Unit4 SaaS

Product Details

Service (or Product)	SKU	Description	Volume Metric	Quantity
Unit4 Enterprise Resource Planning	001-CPK-SA	ERP Core Package	Per FTE Employee	1,500
Unit4 Enterprise Resource Planning	001-FPTUK-SA	Local Finance and Procurement Package - UK	Per FTE Employee	1,500
Unit4 Enterprise Resource Planning	001-PAYPK-SA	Payroll Package	Per FTE Employee	1,500
Unit4 Enterprise Resource Planning	001-PROCPK-SA	Procurement Package	Per FTE Employee	1,500
Unit4 Enterprise Resource Planning	001-PLPK-SA	Projects Base Package	Per FTE Employee	1,500
Unit4 Enterprise Resource Planning	001-STDSER-SA	Standard Support	Per Item	1
Unit4 Enterprise Resource Planning	001-AZUDD-SA	Unit4 Dedicated Cloud	Per Item	1

2. Software Support

Supplier will supply Standard Support Services on the items shown above, as described in the Unit4 Support Terms – Standard Support of the Supplier Terms, available at:
Unit4 General Terms of Business (Dynamic) v.2.1 April 2021 (EN - UKI) (digitalmarketplace.service.gov.uk)

.

Schedule 2: Call-Off Contract charges

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

Unit4 SaaS Charges year 1	[redacted]
Total	= £291,743.99 (excluding VAT)

Unit4 ERP Annual SaaS Charges will have no indexation applied for the initial 12 month period of this Call-Off Contract. For any subsequent years and the optional extension period the Charges will increase by the annual increase in CPI+2, with a minimum of 4%.

.

Schedule 3: Collaboration agreement

NOT REQUIRED

Schedule 4: Alternative clauses

NOT REQUIRED

Schedule 5: Guarantee

NOT REQUIRED

.

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 Clause 2 (Services) 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 Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
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 UK 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 Call-Off Contract and/or actual 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)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK 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.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
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-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
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 RM1557.13 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 Clause 2 (Services) 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.
UK GDPR	The retained EU law version of the 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 ● a Dun & Bradstreet rating of 10 or less
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 Buyer'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, 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.
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 Schedule 6.
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 UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK 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 high performance 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 G-Cloud 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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
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 G-Cloud 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: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

Annex 1: Processing Personal Data

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

Contact Details and Instructions

The contact details of the Buyer's Data Protection Officer are: The Controller address for notices provided in the DPA or Master Agreement.

The contact details of the Supplier's Data Protection Officer are: By email to privacy@unit4.com.

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

Any such further instructions shall be incorporated into this Annex.

Part A - DESCRIPTION OF THE PROCESSING OF PERSONAL DATA

1. Definitions

Capitalised terms used in this Annex shall have the meanings given to them in this Call-Off Contract save as set out below:

1.1	**Data Protection Agreement or DPA**	this Call-Off Contract.
1.2	**Data Protection Authority**	a relevant authority or other body appointed under Data Protection Legislation to monitor and enforce the same.
1.3	**Data Protection Officer or DPO**	the professional, knowledgeable person who advises on and monitors compliance with the Data Protection Legislation and privacy policy within an organization.
1.4	**Schedule**	the data processing information in this Schedule 7 incorporated in this Call-Off Contract.
1.5	**Master Agreement**	the Call-Off Contract.
1.6	**Third Party**	a natural or legal person, a government body, a service or another body, other than the Data Subject, the Controller, the Processor, or the persons authorized under direct authority of the Data Controller or the Processor to Process the Buyer Personal Data.

.

2. Identity of Controller for each Category of Buyer Personal Data

The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Buyer Personal Data recorded below:

Product	**Buyer Personal Data that may be processed might include:**	**To whom this may belong:**
Unit4 ERP x	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.	Current or former employees;
Unit4 ERP 7	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.	Current or former employees;
Unit4 Financials	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.	Current or former employees; Contractors or Sub-contractors (of any variety), agents or directors; and Applicants or prospective employees.
Unit4 FP&A	Names; addresses; telephone numbers (including mobile); email address(es); other contact information. Other Personal Data is not required to be stored or processed to achieve the	Current or former employees;

.

	objectives of the Product (as set out below), but other Personal Data may be stored or processed by the Product if it is configured in such a way to do so (e.g. salary data) or is inputted into the Product by the Customer.	
Unit4 Talent Management	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information (street address and country); date of birth; age; place of birth; job title; department. By using the Learn module: course enrolments; session enrolments; quiz results and reviews; video engagement data; slide engagement data; text engagement data; badges; certifications. By using the perform module: check-in data; OKR data; feedback and praise. By using the Engage module: answers and feedback on engagement questions.	Current or former employees; Current or former job candidates; Contractors or Sub-contractors (of any variety), agents or directors; and Applicants or prospective employees.
People Platform Services ("PPS"), Localisations Services and Unit4 Apps	As the PPS, Localisation Services and/or Unit4 Apps are services that work and interface with Unit4's other Products or Services, they may process any or all types of Personal Data set out in this table in relation to the listed Products and Services.	All categories of individual listed in this table. Depending on the application or service to which Wanda is connected, the PPS could potentially Process Personal Data relating to any living individual that the User chooses to submit.

3. Duration of the Processing

The Processor will keep the Buyer Personal Data for the duration of the Master Agreement.

After the agreed period of retention, the Processor will return the Buyer Personal Data to the Controller, on a migration-capable format set by Processor or immediately destroy the Buyer Personal Data without retaining a copy, upon first request of Controller.

4. Nature and purposes of the Processing

Generally, the nature of the Processing by the Processor will only be as is necessary to enable the Processor to comply with its obligations and exercise its rights under the Master Agreement, including (in relation to the Buyer Personal Data) collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The objective or purpose of the Processing is the performance of the Processors obligations and exercise of its rights under the Master Agreement, including the performance of functions required or requested by the Controller for the Controller's compliance with its statutory and/or contractual obligations. In relation to and depending on the Product or Service. Processor will also Process your Buyer Personal Data to improve her products and services (e.g. for product improvement via artificial intelligence, machine learning etc.) or data analysis. Processing will include the following:

.

Product	Nature and purposes of Processing
Unit4 ERP 7	Buyer Personal Data will be entered into Unit4 ERP 7 to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Travel requests; • Expense claim processing; • Timesheet processing; • Absence management; • HR & Payroll related processes: • Payroll; • Course enrolment; • Competence management; • Appraisals; • Salary review; • Applicant registration; • Payment processing; • Billing; • Purchase requisitions; • People/Project Planning. The Processing will involve: ***Product (software solution)*** Unit4 ERP 7 executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. ***Services*** Transfer and storage of Buyer Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Buyer Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
People Platform Services ("**PPS**"), Localisation Services and/or Apps	Data will be processed by the PPS to permit the stated purposes of the services as set out in the applicable PPS Service Description on www.unit4.com. In addition, Buyer Personal Data will be inputted into Wanda using third party software of choice (e.g. Slack Integration, Facebook Messenger or other Microsoft Applications (including Microsoft Teams)). Dependent on the Unit4 Product or Service used by Customer, Wanda can help to complete administrative tasks for Customer's employees. Tasks may include: • Timesheet entries • Expense entries • Travel requests • Payslip enquiries • Absence entries • Balance enquiries • Purchase requisitions.

.

	The Processing will involve: ***Product (software solution)*** • Wanda executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from Third Party solutions not under the control of the Processor through integrations. ***Services*** • Transfer and storage of Buyer Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. • Access to the Buyer Personal Data to provide support and maintenance of the Unit4 PPS and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. • Access to the Buyer Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. • Access to Buyer Personal Data for product improvement via AI machine learning or data analysis.

5. Description of the Processing and Means

Processer will Process the above Buyer Personal Data in connection with the following activities (the activities below are mentioned as example only):

Type of Processing	**Description**	**Means and resources**
Unit4 SaaS (General)	The Processor will Process Buyer Personal Data in connection with the activities as described in the Master Agreement and more specifically the Unit4 Service Descriptions.	<u>Personnel</u> The Unit4 Cloud operations team has personnel in the EU (including, but not limited to, Poland, Sweden, Norway, Netherlands, Spain and Portugal), UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 SaaS. <u>Assets and Infrastructure</u> Unit4 utilises third party hosting infrastructure services to provide the Unit4 SaaS and employs other software systems for operation and management. See Part C.
Support	The Processor will Process	<u>Personnel</u>

.

Services	Buyer Personal Data in connection with the activities as described in the Master Agreement and more specifically in the Unit4 Support Terms.	The Unit4 Support team has personnel in the EU (including, but not limited to, Poland, Sweden, Norway, Germany, Ireland, Netherlands, Spain and Portugal), UK, US, Canada (and such other locations as required to support Unit4's business needs). These Processor personnel provide the Unit4 Support Services. <u>Assets and Infrastructure</u> Unit4 utilises other software systems for operation, delivery and management of these services.
Professional Services and/or consulting	The Processor will Process Buyer Personal Data in connection with the activities as described in the Master Agreement and more specifically in any more detailed Project documentation or statements of work agreed between the Parties following Project commencement.	<u>Personnel</u> The Unit4 Professional Services team has personnel in all locations where Unit4 has a corporate group entity including United Kingdom, Ireland Poland, Portugal, Norway, Spain, France, Germany Sweden, US, Canada, Singapore/Malaysia (and such other locations as required to support Unit4's business needs). These Processor personnel provide the Unit4 Professional Services. <u>Assets and Infrastructure</u> Unit4 utilises other software systems for operation, delivery and management of these services.
Unit4 Professional Services (if sub-contracted to a delivery partner)	The Processor and its Sub-Processors will Process the aforementioned Buyer Personal Data in connection with the activities as described in the Master Agreement and (if any) the Third Party contractual and service documentation provided as part of the Master Agreement. For more details, See Part C. The Processor will execute a written agreement with the Sub-Processor(s), which will be in accordance with the relevant legislation and regulations and this DPA. Further, the Controller has given the Processor permission to engage the applicable Sub-Processor(s) as listed in Part C by signing this DPA.	See Part C
Third Party Products and Services	The Processor and its Sub-Processors will Process the aforementioned Buyer Personal Data in connection with the	See Part C and any additional provisions provided in further schedules or appendices to this DPA if required by the Third Party Provider or Applicable Law.

.

	activities as described in the Master Agreement and the Third Party contractual and service documentation provided as part of the Master Agreement.	

People Platform Services ("**PPS**"), Localisation Services and/or Apps	In addition to the Unit4 SaaS, the PPS, Localisation Services and/or Apps will (where applicable) process Buyer Personal Data in connection with a privacy statement as presented to the end user, asking for consent, where such Buyer Personal Data is processed.	<u>Personnel</u>
		
		The Unit4 Cloud operations team, which operates the PPS, Localisation Services and/or Apps has personnel in the EU (including, but not limited to, Poland, Sweden, Norway, Netherlands, Spain and Portugal), UK, US, Canada, Malaysia and Singapore. These Processor personnel operate Unit4 SaaS.
		
		<u>Assets and Infrastructure</u>
		
		Unit4 utilises its own and third party (shared) infrastructure services to provide the Unit4 People Platform services, Localisation Services and/or Apps. This includes 3rd party systems (i.e. collaboration apps), over which Unit4 has no control. The PPS including Wanda, Localisation Services and/or Apps make use of a number of Microsoft products and services, as follows:
		• Cognitive services:
		  ○ LUIS Cognitive Service - *language understanding.*
		  ○ Text Translator API – *translating text*
		  ○ QnA Maker Cognitive service – *provides a questions and answers service*
		• Bot framework connectors – *provides for the connection of Wanda to the supported social channels*.
		• Traffic manager – *used for disaster recovery and failover if the primary region is unhealthy*
		• Web apps / web jobs – *hosts web APIs and long running web-based processes*
		• Service bus – *provides internal communication in the Wanda ecosystem*
		• Storage accounts – *used to store conversation state and user settings*
		• Cosmos DB –*provides storage*
		• Key vault – *stores confidential data that is used to communicate with Microsoft services and for internal services*
		• Redis cache – *provides caching capabilities*
		• Application Insights – *Monitoring of system, includes telemetry and logging*
		• *SQL server – provides storage*
		• Kubernetes – *open source container*
		
		Further information and details relating to those Microsoft products and services can be found here: https://azure.microsoft.com/en-

.

		us/services/. Next to that the PPS, Unit4 Localisation Services and/or unit4 Apps make use of: Twilio – sendgrid – to send mail messages

6. Information regarding Country (or Place) of Processing of Buyer Personal Data

<table>
<tr><td>Product - On premises</td><td colspan="4">Data is stored on the servers of the Controller in their principal place of business or registered office as can be notified to Unit4 from time to time.</td></tr>
<tr><td>Product - Unit4 SaaS</td><td colspan="4">Unit4 Cloud operates in several data centres, including a worldwide presence in Microsoft Azure. Unit4 will deploy the customer in the most logical location dependent on where the Customer resides (as set out in an order form). All Customer data will be stored only in the selected geo-political zone and won't be moved outside of it without explicit customer consent.
<table>
<tr><th>CLOUD MODEL</th><th>GEO-POLICITAL ZONE</th><th>LOCATION OF DATA CENTRE</th><th>FACILITY OR PARTNERSHIP</th></tr>
<tr><td>SAAS CLOUD</td><td>EU</td><td>DUBLIN / AMSTERDAM</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>UNITED KINGDOM</td><td>LONDON / CARDIFF</td><td>MICROSOFT AZURE</td></tr>
</table></td></tr>
<tr><td>Unit4 Support – Standard Support and other standard support services</td><td colspan="4">Unit4 Support uses third party software (such as salesforce / ServiceNow) to register and process Cases. These Cases are accessible for any Unit4 employee that is provided access to third party software such as support engineers, cloud engineers, Professional Services consultants and service management. Access is controlled by internal management and organisational processes, to ensure that Buyer Personal Data is not accessed by consultants or engineers in locations that should not have access to particular Customer details.
<table>
<tr><th>Customer Location</th><th>Primarily Support is provided from:</th></tr>
<tr><td>United Kingdom and Ireland</td><td>United Kingdom, Ireland, Portugal and Poland.</td></tr>
<tr><td>Sweden, Norway, Denmark, Finland and Iceland</td><td>Poland, Portugal, Norway and Sweden.</td></tr>
<tr><td>US & Canada</td><td>Poland, Portugal, US and Canada.</td></tr>
<tr><td>Europe rest</td><td>Poland, Portugal and Germany.</td></tr>
<tr><td>APAC</td><td>Poland, Portugal and Singapore/ Malaysia.</td></tr>
</table></td></tr>
<tr><td>Unit4 Support – 24/7 Support</td><td colspan="4">Using a 'follow the sun' methodology, 24/7 support of Customer Cases could occur in any of the support locations listed above as well as Netherlands, Spain and such other locations as required to support Unti4's business needs.</td></tr>
<tr><td>Unit4 Support – EU Only Support</td><td colspan="4">If EU Only support is elected, Cases are supported only within the EU locations listed above for standard support (during Business Hours).</td></tr>
<tr><td>People platform services ("PPS") (generally) including IDS and Wanda</td><td colspan="4">PPS are cloud services that use shared infrastructure and 3rd party services that might not provide geopolitical zone isolation. Below is an overview of the PPS and the country (or place) of Processing of Buyer Personal Data using that service.</td></tr>
</table>

.

(together with any supporting services), localisation services and/or apps	**Service**	**Geo-political zone**	**Where Service Processes or Stores Data**	**Primarily Support is provided from:**
	Wanda	Any	Predominantly within the EU, but can be anywhere globally where there is an Azure data centre (e.g. US).	EU countries including Ireland, Poland and Spain, United States and other Global support locations where required.
	PPS, Localisation Services and/or Apps	Depends on Cloud Deployment	Service is processed and data is stored in the selected Geo-Political zone.	As above for Unit4 SaaS
Unit4 Professional Services and Unit4 customer success function	**Topic**	**Professional Services and customer success are provided from:**		
	Implementation and other project services	In the Territory or Customer location of registered office/principal place of business (as applicable) and/or Portugal depending on what is agreed between the Parties in the project documentation or a statement of work (if applicable).		
	Data Migration	In the Territory or Customer location of registered office/principal place of business (as applicable) and/or Portugal depending on what is agreed between the Parties in the project documentation or a statement of work (if applicable).		
	Trouble shooting	In applicable Unit4 Support Service location and Portugal.		
	Customer Success	In applicable Unit4 Support Service location and Portugal.		

.

PART B - SECURITY MEASURES

As stated in the Master Agreement, the technical and organisational security measures are listed in this Part and are supplemented or amended if necessary. The Controller considers these measures suitable for the processing of Personal Data.

Unit4 Business Security Measures (Internal business operations summary)

Description of the technical and organisational security measures implemented by the Processor in its organisation (generally):

Physical Security:

- Physical access control is managed by Unit4 facilities.
- All offices have security systems in place in respect of controlling access through barriers, e.g. entry gates, manned reception desks, alarmed fire doors, intruder detection systems and/or lockable offices.
- Unit4 operates access controls with the help of what people know, such as password or personal access code; or with the help of what people carry, such as a security pass;
- On-site server rooms (where applicable) have additional physical controls.
- Access to secure areas or sensitive information is restricted to prevent unauthorized access by visitors / unauthorized staff (by way of lockable offices or lockable cabinets) and operating clear desk policies where appropriate.
- Unit4 visitors are controlled at reception (whether by a dedicated receptionist or other member of staff).
- Shredders or other suitable secure disposal method for sensitive documents are used.

Virtual and computing Security:

The responsible line manager will ensure employees and contractors return all Unit4 assets in their possession upon termination of their employment or contract agreement. Records of this return of asset are maintained.

- Unit4 aims to classify information as either public, confidential, proprietary or sensitive. Information would then be protected according to its classification.
- Media (including hard drives) are disposed of securely and safely when no longer required. All sensitive material (hard disks, floppies, etc.) is removed by guaranteed removal software, (not by reformatting or deletion) before disposal or physical destruction.
- Anti-malware - we use the latest version of industry standard solutions to provide virus and anti-malware protection.
- Further, Unit4 utilises:
    - control on assigned rights;
    - logging and controlling access to the system;
    - recovery measures;
    - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Pro cessing systems and services; and
    - systems and processes to allow it to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- Business Continuity and Disaster Recovery plans have been prepared which include information security considerations.

Security Policies and Documentation:

- The Global Leadership Team for Unit4 and/or its respective local management teams have oversight of both global and local information management and security plans including any information security policies that meet identified information security risks and supports the business goals.
- Information security and management is assigned globally to the Chief Information Security Officer and Global Data Protection Officer, who manage resources to deliver strategic and overall

.

compliance with information security policy and process.

- Unit4 has implemented security policies updated and amended regularly to comply with good industry practice.
- Unit4 has a privacy policy and white paper on GDPR published on www.unit4.com/terms.
- Unit4 enters into non-disclosure and confidentiality agreements with Third Parties when sharing confidential information relation to its business.
- Unit4 ensures all employees and contractors enter into standard confidentiality clauses in their contracts.
- Unit4 provides all employees with training in relation to: data protection; security and its core business principles as stated above.

Additional Elements for Unit4 SaaS on Microsoft Azure (summary)

Description of the technical and organisational security measures implemented by the Processor in relation to the provision of the Unit4 SaaS:

Data protection

Unit4 Cloud utilizes several mechanisms to protect Personal Data in the cloud. Below is a comprehensive overview of applied controls.

Network level security features, process and protocols

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
- System security – Logical authentication and authorization mechanism in place
- Firewalls – next generation firewall technology to ensure inbound and outbound traffic is controlled.

Database level security features, process and protocols

- Data security – Logical authentication and authorization mechanism in place.
- Database security – Every customer has their own secure database which means partitioning of databases is not required and customer data not co-mingled. The outcome is that a customer's data is never inadvertently shared with others.
- Database backups are encrypted using whole database encryption technology such as Transparent Database Encryption.
- Non-transactional data and files will be secured by standard symmetric encryption (AES).
- Unit4 uses Azure Key Vault to maintain control of keys used by cloud applications and services to encrypt data.

Continually tested and evolving security

To uncover unforeseen vulnerabilities and refine our detection and response capabilities, we are continually looking into how we can improve out security posture to defend against potential breaches. The Unit4 Cloud operations team that closely monitor and secures Unit4's Cloud operations (cloud infrastructure, cloud services, products, devices and internal resources) — testing penetration and improving our ability to protect, detect and recover from cyber threats.

Threat detection, mitigation and response

As the number, variety and severity of cyber threats have increased, so has our diligence in threat detection and response. Centralized monitoring systems provide continuous visibility and timely alerts. Frequent application of security patches and updates helps protect systems from known vulnerabilities. Intrusion and malware detection systems are designed to detect and mitigate risks from outside attacks. In the event of malicious activity, our incident response team follows established procedures for incident management, communication and recovery. The team uses industry best practices to alert both internal

.

teams and customers. Finally, security reports monitor access patterns to help proactively identify and mitigate potential threats.

Data segregation

Data is the currency of the digital economy and we take the responsibility of protecting customer data very seriously. Both technological safeguards, such as encrypted communications and operational processes help keep customer data secured. In the Cloud, data from multiple customers may be stored on the same IT resources. Unit4 uses logical isolation to segregate each customer's data from that of others. Unit4 SaaS is designed to counter risks inherent in a multitenant environment. Data storage and processing is logically separated among consumers having separate database instances for all our customers.

Data encryption

Unit4 provides, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks. This is done by using only secure protocols, like HTTPS over TLS, using latest security ciphers. The mechanism used is a transparent, whole database encryption – TDE. Microsoft Azure customers in the Public SaaS offering get the TDE data at rest encryption as a standard.

Access control

Customers using Unit4 products in the Cloud are fully empowered to conduct front-end access control to their application. This means that the responsibility for creating new accounts, account termination and review for Unit4 application is with the customer.

Unit4 will retain limited back-end access to customer data (by direct database connection). Access by Unit4 to Personal Data shall be strictly limited to activities necessary for installing, implementing, maintaining, repairing, troubleshooting or upgrading the solution. All access is logged and limited to a small group of Cloud Engineers and Support Consultants. Access logs are saved in the centralized monitoring solution for 365 days. In case of data breaches, Unit4 can provide the access log on request.

Data breach notification

Unit4 shall notify the Customer without undue delay after becoming aware of a data breach. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

Data privacy and security by design

Unit4 Cloud platform was designed from the ground up with data security and privacy in mind. Unit4 is continually improving the security of the solution, by applying lessons learned from annual penetration tests and audits.

Unit4 and the data centres operators hold various security certifications, for the details please refer to the applicable Service Description.

Additional Elements for Unit4 People Platform Services (summary)

Description of the technical and organisational security measures implemented by the Processor in relation to the provision of the Unit4 People Platform Services (Cloud only):

Data protection

Unit4 People Platform utilizes several mechanisms to protect Personal Data in the cloud. Below is a comprehensive overview of applied controls.

Network level security features, process and protocols

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.

.

Authentication

- All services follow the principle of least privilege and authentication towards services and their APIs are secured using industry standard mechanisms. OpenID Connect and the underlying oAuth 2.0 protocol is used to securely perform authentication of users and/or client services with trusted parties and validate identity and access using claims-based tokens.
- HMAC (Hash-based Message Authentication) is used as alternative method to secure communication between services.

Database level security features, process and protocols

- A data stored in storage accounts are encrypted at rest.
- All storage accounts require secure transfer – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
- All data stored in Azure Cosmos DB is encrypted at rest and in transport.
- All Azure SQL Servers are enabled with Transparent Data Encryption (TDE).
- All Azure SQL Servers are running with Threat detection and auditing enabled.
- Azure KeyVault is used to secure particular sensitive information like service principal credentials.

Messaging level security features, process and protocols.

- All data stored by Azure Service Bus instances are encrypted at rest.
- All traffic (in transit) on the Azure Service Bus is secured using industry standard protocols such as SSL

More details about the Security Policy and Security Program can be found at www.unit4.com/terms.

Data encryption

Unit4 People Platform services provide, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks. This is done by using only secure protocols, like HTTPS over TLS (1.2), using latest security ciphers. All data stored are encrypted.

Data breach notification

Unit4 shall notify the Customer without undue delay after becoming aware of a data breach. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

Data privacy and security by design

Unit4 People Platform services were designed from the ground up with data security and privacy in mind. Unit4 is continually improving the security of the solution, by applying lessons learned from annual penetration tests and audits.

.

PART C – SUB-PROCESSORS

Service	**Sub-Processor** (company name, location etc.)	**Processing location**	**Type of service by Sub-Processor / Module used with**
Unit4 Professional Services (if sub-contracted to a delivery partner)	As specified in the Master Agreement.	As specified in the Master Agreement.	As specified in an order form or agreed in writing with Customer.
Third Party Products and Services only applicable when purchased by customer	As specified in the Master Agreement.	As provided in the Master Agreement or in any further schedules or appendices to the Agreement relating to the Third Party Provider processing.	Software and//or Support Services and/or Cloud Services.
Unit4 SaaS	Microsoft Azure	As stated above in Part A, paragraph 3.	Providing Cloud Infrastructure and Services
	Microsoft Dynamics	As stated above in Part A, paragraph 3.	Providing Software Services, in particularly Microsoft Dynamics (including some cloud infrastructure).
	Microsoft	As stated above in Part A, paragraph 3.	Providing software tooling and Office
	Conapto	As stated above in Part A, paragraph 3.	Providing Cloud Infrastructure and Services
	Twilio - Sendgrid	United States of America (Privacy Policy)	Sending mail
People Platform Services ("**PPS**") (generally) including IDS and Wanda (together with any supporting services)	Microsoft Azure	As stated above in Part A, paragraph 3 and as provided by Microsoft here: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located.	Providing Cloud Infrastructure and platform Services (as set out above) in Part A.
	Twilio - Sendgrid	United States of America (Privacy Policy)	Sending mail