Crown Commercial Service

G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

G-Cloud 14 Call-Off Contract

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	164362055695264
Call-Off Contract reference	CQC HWE 28
Call-Off Contract title	Engagement Platform
Call-Off Contract description	Healthwatch England Facebook Workplace Replacement to Workvivo via Zoom Communications Inc. Annual Subscription and Migration Services
Start date	30/04/2025
Expiry date	29/06/2027
Call-Off Contract value	£54,264.00 (over 2 years Paid Period) VAT Not Applicable. See Call-Off Charges breakdown table below.
Charging method	Invoice – BACS Annually in advance
Purchase order number	TBC

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

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	Care Quality Commission on Behalf of Healthwatch England Citygate, Gallowgate Newcastle upon Tyne NE1 4PA
To the Supplier	Zoom Communication Inc. (a Delaware corporation with file number 4969967) Telephone: (888) 799-9666 Supplier's address: 55 Almaden Boulevard, Suite 600, San Jose, CA 95113, USA

Together the 'Parties'

Principal contact details

For the Buyer:

Title: Director of Communications Insight and Campaigns

Name: [redacted]

Email: [redacted]

Phone: [redacted]

For the Supplier:

Title: Account Executive

Name: [redacted]

Email: [redacted]

Phone: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract commences on 30 April 2025 with a Free Period of two (2) months commencing on 30 April 2025 and the Paid Period commencing on 30 June 2025 which shall then continue for 24 months.

Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of 30 working days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for two periods of up to 12 months, by giving the Supplier 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. The Year 3 and Year 4 extensions are subject to external approval via the DHSC NHSX Digital and Technology Assurance Spend Control Process.

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	Provide employee experience app as outlined below and in Schedule 1 ● Employee communications ● Employee experience ● Employee engagement ● Social intranet
Additional Services	**Not Applicable**
Location	The Services will be delivered to: ● [redacted] ● Remotely (Supplier staff will access systems from home) and/or Workshops will be conducted either in person or virtually via Microsoft Teams or skype (or similar).
Quality Standards	The quality standards required for this Call-Off Contract are as provided in the service description as listed on the Digital Marketplace.
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are as provided in the service description as listed on the Digital Marketplace.
Service level agreement:	The Service Levels and availability criteria required for this Call-Off Contract are as stated in Supplier's service description listed on the Digital Marketplace.

Onboarding	Not applicable

Offboarding	The offboarding plan for this Call-Off Contract will be agreed with the Supplier and Buyer within one month of the Call-Off Contract start date. End-of-contract data extraction Upon request by Buyer made within thirty (30) days after the effective date of termination or expiration of the G Cloud 14 Call-Off, The Supplier will make the Buyer Data available in an agreed Extract format to Buyer through the Service at no additional cost. Call-Off Contract Clause 21 (Exit Plan) and Clause 10 (Termination and consequences of termination) apply.
Collaboration agreement	Not Applicable

Limit on Parties' liability	Defaults by either party resulting in direct loss or damage 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 125% of the total contract value. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed 125**%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other Defaults will not exceed the greater of 125**%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Buyer's responsibilities	Not applicable
Buyer's equipment	Not applicable.

Supplier's information

Subcontractors or partners	Not applicable

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: Annually in advance.
Invoice details	The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Invoices will be sent via email to: [redacted]
Invoice information required	All invoices must include the relevant purchase order number.
Invoice frequency	Invoice will be sent to the Buyer annually.
Call-Off Contract value	The total value of this Call-Off Contract is £108,528.00 (VAT not applicable).

Call-Off Contract charges	The breakdown of the Charges is: • [redacted] **Engagement Platform** / **Cost per annum** / **Subtotal** / **Total over 4 years (Paid Period)** [redacted] **Total for 4 years (Paid Period). (if Term is extended) (VAT not applicable)** — **£108,528.00**

Additional Buyer terms

Performance of the Service	This Call-Off Contract must adhere to the quality standards and services as described in the service description as listed on the Digital Marketplace.

Guarantee	Not applicable
Warranties, representations	All Warranties and representations are as per Clause 2.3 of the Framework Agreement.
Supplemental requirements in addition to the Call-Off terms	Not applicable
Alternative clauses	Not applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not applicable.
Personal Data and Data Subjects	As described in Annex 1 of Schedule 7.
Intellectual Property	Please see Clause 11 in this Call-Off Contract as well as Clause 27 of the Framework Agreement
Social Value	Not applicable

Performance Indicators	N/A

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 clauses 8.3 to 8.6 inclusive 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 RM1557.14.

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

Call-Off Contract Signatures

IN WITNESS of which this Contract has been duly executed by the parties.

SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:

SIGNED for and on behalf of **ZOOM COMMUNICATIONS INC.**

Authorised Signatory 1:

Authorised Signatory 2:

Buyer Benefits

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

G-Cloud 14 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 36 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules 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)
5.4 to 5.6 (Change of control)
5.7 (Fraud)
5.8 (Notice of fraud)
7 (Transparency and Audit)
8.3 to 8.6 (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)

30 (Insurance)
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

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

a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

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.

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

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 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

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

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

5. Due diligence

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

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

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

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

5.1.4 have entered into the Call-Off Contract relying on 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

9.2.3all 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

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 trademarks 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:
alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;
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 judgement 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:

rights granted to the Buyer under this Call-Off Contract

Supplier's performance of the Services

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:

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

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

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:

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

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-security-classifications

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

18.5A 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

18.5.2an 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:

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

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

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

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

work with the Buyer on any ongoing work

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

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.

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 CDDO 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

21.6.4it 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 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

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 24.5 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 is not a 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.

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.

The Supplier will cooperate 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.

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

its failure to comply with the provisions of this clause

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

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

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 using the template in Schedule 9 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 using the template in Schedule 9. 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. [redacted]

2. [redacted]

. [redacted]

[redacted]

[redacted]

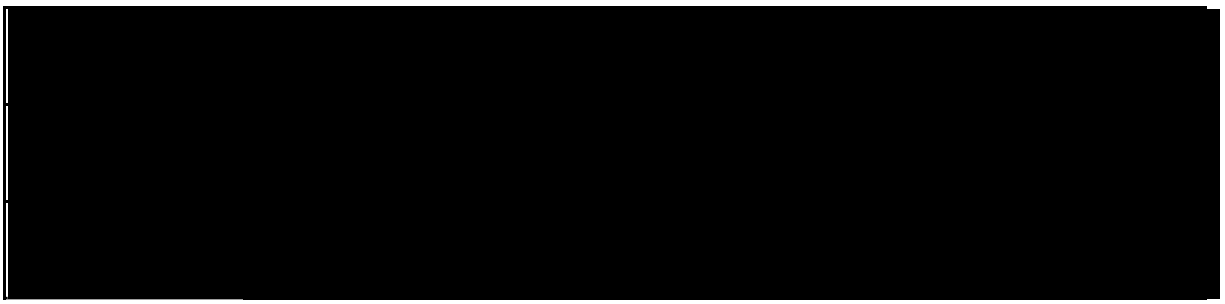
3. [redacted]

4. [redacted]

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) can't be amended during the term of the Call-Off Contract.

Clause 3 and Schedule 4 of the Framework Agreement apply.



Schedule 3: Collaboration agreement – Not Used

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Buyer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Buyer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

Employment (Northern Ireland) Order 2002
Fair Employment and Treatment (Northern Ireland) Order 1998
Sex Discrimination (Northern Ireland) Order 1976 and 1988
Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
Equal Pay Act (Northern Ireland) 1970
Disability Discrimination Act 1995
Race Relations (Northern Ireland) Order 1997

Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
Employment Equality (Age) Regulations (Northern Ireland) 2006
Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
The Disability Discrimination (Northern Ireland) Order 2006
The Employment Relations (Northern Ireland) Order 2004
Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
Employment Relations (Northern Ireland) Order 2004
Work and Families (Northern Ireland) Order 2006

and will use its best endeavours to ensure that in its employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract it promotes equality of treatment and opportunity between:

persons of different religious beliefs or political opinions
men and women or married and unmarried persons
persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
persons of different ages
persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Buyer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

the issue of written instructions to staff and other relevant persons
the appointment or designation of a senior manager with responsibility for equal opportunities
training of all staff and other relevant persons in equal opportunities and harassment matters
the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Buyer as soon as possible in the event of:

- the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Term by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Buyer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Buyer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Buyer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Buyer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Buyer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Buyer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Buyer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Buyer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Buyer premises, the Supplier will comply with any health and safety measures implemented by the Buyer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Buyer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Buyer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Buyer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Buyer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).

2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee – Not Applicable

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-to-date 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.
Financial Metrics	The following financial and accounting measures: Dun and Bradstreet score of 50 Operating Profit Margin of 2% Net Worth of 0 Quick Ratio of 0.7

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 RM1557.14 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 Supplier Trigger Event
Intellectual Property Rights or IPR	Intellectual Property Rights are: (a) 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 (b) 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 (c) 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, judgement 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, judgement, 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.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
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 and Performance Indicators 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-controlsche ck-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.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	An assessment of the impact of a variation request by the Buyer completed in good faith, including: details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract; details of the cost of implementing the proposed variation; details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; a timetable for the implementation, together with any proposals for the testing of the variation; and such other information as the Buyer may reasonably request in (or in response to) the variation request;

Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Intentionally Blank

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.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: [redacted], Data Protection Officer, Governance and Legal Services, Care Quality Commission, Citygate, Gallowgate, Newcastle upon Tyne, NE1 4PA, United Kingdom. Email: [redacted]

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [redacted]

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

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

Description	Details
Identity of Controller and Processor for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: For more information on how the Supplier processes Personal Data, please refer to the Data Processing Addendum incorporated herein as Schedule 10
Duration of the Processing	For the duration of the Call-Off Contract
Nature and purposes of the Processing	As described in the Data Processing Addendum incorporated herein as Schedule 10.
Type of Personal Data	As described in the Data Processing Addendum incorporated herein as Schedule 10

Categories of Data Subject	As described in the Data Processing Addendum incorporated herein as Schedule 10
International transfers and legal gateway	Data storage and processing locations European Economic Area (EEA) As described in the Data Processing Addendum incorporated herein as Schedule 10
Plan for return and destruction of the data once the Processing is complete	As described in the Data Processing Addendum incorporated herein as Schedule 10

Annex 2 - Joint Controller Agreement – Not applicable

Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.
1.2 The Parties agree that the [**select: Supplier or Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for using all reasonable endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**select:** Supplier's **or Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

1.1.2.1 The Supplier and Buyer each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Framework Agreement during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Framework Agreement or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) use all reasonable endeavours to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

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

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

(k) where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs ("the **Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

(l) where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the transfer is in accordance with Article 45 of the EU GDPR; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) the transferring Party complies with its obligations under EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

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

3. Data Protection Breach

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

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including using such reasonable endeavours as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the

Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

1.1.4.1 The Supplier shall permit:

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

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

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

5. Impact Assessments

1.1.5.1 The Parties shall:

provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

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

6. ICO Guidance

The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Framework Agreement to ensure that it complies with any guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority.

7. Liabilities for Data Protection Breach

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

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

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

if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

1.1.7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable,

the liability will be apportioned between the Parties in accordance with the decision of the Court.

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

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

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

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

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Framework Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

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

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Framework Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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

Schedule 8 - Corporate Resolution Planning - Not applicable

Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	**[insert** name of Buyer] **("the Buyer")** And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
A Variation Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: **[Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

Words and expressions in this Variation shall have the meanings given to them in the Contract.

The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature .....

Date .....

Name (in Capitals) .....

Address .....

Schedule 10 – Data Processing Addendum

This Data Processing Addendum, including its Exhibits (this "**Addendum**"), forms part of the Master Subscription Agreement, Terms of Service, Terms of Use, or any other agreement about the delivery of the contracted services between Zoom Communications, Inc. ("**Zoom**") and the Customer (the "**Agreement**") named in such Agreement or identified below to reflect the parties' agreement about the Processing of Customer Personal Data (as those terms are defined below).

In the event of a conflict between the terms and conditions of this Addendum, the Agreement, an Order Form, or any other documentation, the terms and conditions of this Addendum govern and control with respect to the subject matter of Processing of Customer Personal Data. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "**Affiliate**" means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party. For purposes of this Addendum, "**control**" means an economic or voting interest of at least fifty percent (50%) or, in the absence of such economic or voting interest, the power to direct or cause the direction of the management and set the policies of such an entity.

1.2 "**Anonymised Data**" means, having regard to the guidance published by the European Data Protection Board, Personal Data which does not relate to an identified or identifiable natural person or rendered anonymous in such a manner that the data subject is not or no longer identifiable.

1.3 "**Applicable Data Protection Law**" means any applicable legislative or regulatory regime enacted by a recognized government, or governmental or administrative entity with the purpose of protecting the privacy rights of natural persons or households consisting of natural persons, in particular the General Data Protection Regulation 2016/679 ("**GDPR**") and supplementing data protection law of the European Union Member States, the United Kingdom's Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Swiss Federal Data Protection Act ("**Swiss DPA**"), Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**") S.C. 2000, ch. 5, and any provincial legislation deemed substantially similar to PIPEDA under the procedures set forth therein, the Brazilian Law No. 13,709/2018 - Brazilian General Data Protection Law ("**LGPD**"), the ePrivacy Directive 2002/58/EC (the "**Directive**"), together with any European Union Member national implementing the Directive.

1.4 "**Authorized Subprocessor**" means a subprocessor engaged by Zoom to Process Customer Personal Data on behalf of the Customer per the Customer's Instructions under the terms of the Agreement and this Addendum. Authorized Subprocessors may include Zoom Affiliates but shall exclude Zoom employees, contractors and consultants.

1.5 "**Controller**" means the entity that determines as a legal person alone or jointly with others the purposes and means of the Processing of Personal Data.

1.6 "**Customer Personal Data**" means Personal Data, including but not limited to:

(a) Content Data: All text, sound, video, or image files that are part of an End User's profile and End User information exchanged between End Users (including guest users participating in Customer-hosted meetings and webinars) and with Zoom via the Services;

(b) Account Data (name, screen name and email address);

(c) Support Data (as defined in Annex I of the Standard Contractual Clauses);

(d) Website access Data (including cookies); and

(e) Diagnostic Data, including but not limited to: Data from applications (including browsers) installed on End User devices ("**Telemetry Data**"), Service generated server logs (for example meeting metadata and End User settings) and internal security logs that are generated by or provided to Zoom by, or on behalf of, Customer through use of the Services as further defined in in Annex I of the Standard Contractual Clauses).

1.7 **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.

1.8 **"Legitimate Business Purposes"** means the exhaustive list of specific purposes for which Zoom is allowed to process some Personal Data as a Controller as specified in Section 2.4.

1.9 **"Personal Data"** means any information relating to a Data Subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes any special categories of Personal Data defined in Art. 9 of the UK GDPR, data relating to criminal convictions and offences or related security measures defined in Art. 10 of the UK GDPR and national security numbers defined in Art. 87 of the GDPR and national supplementing law.

1.10 **"Processor"** means the entity that processes Personal Data on behalf of the Controller.

1.11 **"Personal Data Breach"** means a breach of security which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data Processed by Zoom or Zoom's Authorized Subprocessor.

1.12 **"Process"** or **"Processing"** means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. For the avoidance of doubt: This includes processing of Personal Data to disclose, aggregate, pseudonymise, de-identify or anonymize Personal Data, and to combine Personal Data with other Personal Data, or to derive any data or information from such Personal Data.

1.13 **"Services"** means the Zoom Services as set forth in the Agreement or associated Zoom order form.

1.14 **"Specific US State Data Protection Law**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any regulations promulgated thereunder ("**CCPA**"); the Colorado Privacy Act of 2021; the Virginia Consumer Data Protection Act of 2021; the Utah Consumer Privacy Act of 2022, as amended; and any other US state law that may be enacted that adheres to the same or substantially the same requirements of the aforementioned laws in this definition.

1.15 **"Standard Contractual Clauses"** means: (i) where the GDPR applies the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "**EU SCCs**"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") (the **"Swiss SCCs**").

1.16 **"Supervisory Authority"** means an independent public authority responsible for monitoring the application of Applicable Data Protection Law, including the Processing of Personal Data covered by this Addendum.

2. Processing of Personal Data: Roles, Scope and Responsibility

2.1 The parties acknowledge and agree to the following: Customer is the Controller of Customer Personal Data. Zoom is the Processor of Customer Personal Data, except where Zoom or a Zoom Affiliate acts as a Controller processing Customer Personal Data in accordance with the exhaustive list of Legitimate Business Purposes in Section 2.4.

2.2 Only to the extent necessary and proportionate, Customer as Controller instructs Zoom to perform the following activities as Processor on behalf of Customer:

(a) Provide and update the Services as configured, and used by Customer and its users, (for example, through Customer's use of Zoom settings or administrator controls) including to make ongoing product improvements and provide personalised experiences and recommendations;

(b) Secure and real-time monitor the Services;

(c) Resolve issues, bugs, and errors;

(d) Provide Customer requested support, including applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymized; and

(e) Process Customer Personal Data as set out in the Agreement and Annex I to the Standard Contractual Clauses (subject matter, nature, purpose, and duration of Personal Data Processing in the controller to processor capacity and any other documented instruction provided by Customer and acknowledged by Zoom as constituting instructions for purposes of this Addendum.

(collectively, the "**Instructions**").

2.3 Zoom shall immediately notify the Customer, if, in Zoom's opinion, an Instruction of the Customer infringes Applicable Data Protection Law and request that Customer withdraw, amend, or confirm the relevant Instruction.

Pending the decision on the withdrawal, amendment, or confirmation of the relevant Instruction, Zoom shall be entitled to suspend the implementation of the relevant Instruction.

2.4 Zoom may Process certain Customer Personal Data for its own Legitimate Business Purposes, as an independent Controller, solely when the Processing is strictly necessary and proportionate, and if the Processing is for one of the following exhaustive list of purposes:

(a) Directly identifiable data (name, screen name, profile picture and email address and all Customer Personal Data directly connected to such directly identifiable data) may be Processed for:

(i) billing, account, and Customer relationship management (marketing communications to procurement, sales, and other Customer personnel that requests such communication), and related Customer correspondence (mailings about for example necessary updates);

(ii) complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data processed by Zoom as data Controller (for example website data), tax requirements, agreements and disputes;

(iii) abuse detection, prevention, and protection (such as automatic scanning for matches with identifiers of known Child Sexual Abuse Material ("**CSAM**")), virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Zoom´s Acceptable Use Guidelines;

(b) Pseudonymized and/or aggregated data (Zoom will pseudonymise and/or aggregate as much as possible and pseudonymized and/or aggregated data will not be processed on a per-Customer level), for:

(i) improving and optimizing the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of the Services, including zoom.us, explore.zoom.us, and support.zoom.us;

(ii) internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including product strategy); and

(iii) receiving and using Feedback for Zoom's overall service improvement.

When acting as an independent Controller, Zoom will not process Customer Personal Data for any purposes other than the above list of Legitimate Business Purposes.

2.5 Zoom will not Process Customer Personal Data for third-party advertising, direct marketing, profiling, research or analytics purposes except where such processing is (i) necessary to comply with Customer's instructions as set out in Section 2.2 of this Addendum, or (ii) for the Legitimate Business Purposes described in Section 2.4 or (iii) part of Zoom's free Services, early access program, or beta program.

2.6 Zoom shall only process Customer Personal Data for the purposes specified in this Addendum; provided, however, Zoom may process Customer Personal Data for "further" or "compatible" purposes (within the meaning of Articles 5(I)(b) and 6(4) GDPR, where applicable), or seek consent from End Users for new types of data processing, where permitted by the Zoom account administrator and Applicable Data Protection Law.

2.7 With regard to content scanning for CSAM and reporting 'hits' to The National Center for Missing & Exploited Children ("**NCMEC**"), Zoom will conduct human review of matched content before it is reported. Zoom may immediately suspend the account of the End User and if legally allowed to do so, notify the End User thereafter of the suspension and the option to appeal the suspension if applicable.

2.8 Regardless of its role as Processor or Controller, Zoom shall process all Customer Personal Data in compliance with Applicable Data Protection Laws, the "Security Measures" referenced in Section 6 of this Addendum and Annex I to the Standard Contractual Clauses.

2.9 Customer shall ensure that its Instructions to Zoom comply with all laws, rules, and regulations applicable to Customer Personal Data, and that the Processing of Customer Personal Data per Customer's Instructions will not cause Zoom to be in breach of Applicable Data Protection Law. Customer is solely responsible for the accuracy, quality, and legality of (i) the Customer Personal Data provided to Zoom by or on behalf of Customer; (ii) how Customer acquired any such Customer Personal Data; and (iii) the Instructions Customer provides to Zoom regarding the Processing of such Customer Personal Data. Customer shall not provide or make available to Zoom any Customer Personal Data in violation of the Agreement, this Addendum, or otherwise in violation of Zoom's Acceptable Use Guidelines (currently published at https://explore.zoom.us/en/community-standards/ as updated from time to time) and shall indemnify Zoom from all claims and losses in connection therewith.

2.10 Following the completion of the Services, at Customer's choice, to the extent that Zoom is a Processor, Zoom shall either enable Customer to delete some of Customer's Personal Data (for example an End User's Personal Data) or all of Customer's Personal Data, shall return to Customer the specified Customer Personal Data, or shall delete the specified Customer Personal Data, and delete any existing copies in compliance with its data retention and deletion policy. If return or destruction is impracticable or incidentally prohibited by a valid legal order law, Zoom shall take measures to inform the Customer and block such Customer Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by applicable law) and shall continue to appropriately protect the Customer Personal Data remaining in its possession, custody, or control and, where any Authorized Subprocessor continues to possess Customer Personal Data, require the Authorized Subprocessor to take the same measures that would be required of Zoom.

3. Privacy by design and by default

3.1 Zoom agrees to minimize Processing to the extent necessary to provide the Services and for the purposes permitted in this Addendum, the Agreement, or as otherwise agreed upon by Customer and Zoom. This includes minimization of Telemetry Data, Support Data, and feedback functionality; minimization of data retention periods; collection of pseudonymised identifiers when necessary, but immediate effective (irreversible) anonymization when the Service can be performed without Personal Data; and the implementation and control of strict access controls to the Customer Personal Data.

3.2 Zoom shall maintain a process whereby when Zoom collects new types of Diagnostic Data, such new collection shall be supervised by a privacy officer. Zoom will perform regular checks on the contents of collected Telemetry Data to verify that neither directly identifying data are collected nor Customer Content Data.

3.3 Regarding Zoom's use of cookies or similar tracking technology, Zoom shall ensure that only those cookies which are strictly necessary shall be set by default for European Enterprise and Education Customers on zoom.us, support.zoom.us, and explore.zoom.us, including visits to these pages when the End User or system administrator has signed into the Zoom account.

3.4 When Zoom plans to introduce new features, or related software and services ("**New Service**"), which will result in new types of Processing (i.e., new Personal Data and/or new purposes), Zoom will:

(a) perform a data protection impact assessment;

(b) determine if the new types of Processing following a New Service are allowed within the scope of this Addendum; and

(c) ensure that the new Processing occurs with the necessary Customer notice or consents.

4. Authorized Persons

Zoom shall ensure that all persons authorized to Process Customer Personal Data and Customer Content are made aware of the confidential nature of Customer Personal Data and Customer Content and have committed themselves to confidentiality (e.g., by confidentiality agreements) or are under an appropriate legal obligation of confidentiality.

5. Authorized Subprocessors

To the extent that Zoom is a Processor:

5.1 Customer hereby generally authorizes Zoom to engage subprocessors in accordance with this Section 5.

5.2 Customer approves the Authorized Subprocessors listed at https://explore.zoom.us/docs/en-us/subprocessors.html:

5.3 Zoom may remove, replace, or appoint suitable and reliable further subprocessors in accordance with this Section 5.3:

(a) Zoom shall at least thirty (30) business days before the new subprocessor starts processing any Customer Personal Data notify Customer of the intended engagement (including the name and location of the relevant subprocessor, and the activities it will perform and a description of the Personal Data it will process). To enable such notifications, Customer shall visit https://explore.zoom.us/docs/en-us/subprocessors.html and enter its desired and valid email address into the submission field at the bottom of the webpage, and Zoom shall send such notifications to the email address entered into the submission field.

(b) In an emergency concerning Service availability or security, Zoom is not required to provide prior notification to Customer but shall provide notification within seven (7) business days following the change in subprocessor.

In either case, Customer may object to such an engagement in writing within fifteen (15) business days of receipt of the aforementioned notice by Zoom.

5.4 If Customer objects to the engagement of a new subprocessor, Zoom shall have the right to cure the objection through one of the following options (to be selected at Zoom's sole discretion):

(a) Zoom cancels its plans to use the subprocessor with regard to Customer Personal Data.

(b) Zoom will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the subprocessor with regard to Customer Personal Data.

(c) Zoom may cease to provide, or Customer may agree not to use (temporarily or permanently), the particular aspect of the Service that would involve the use of such a subprocessor with regard to Customer Personal Data.

(d) Zoom provides Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If Zoom, in its sole discretion, cannot provide any such alternative(s), or if Customer does not agree to any such alternative(s), if provided, Zoom and Customer, within thirty days (30) days of being provided an alternative, may terminate the affected portion(s) of the Agreement with prior written notice. Termination shall not relieve Customer of any fees or charges owed to Zoom for Services provided up to the effective date of the termination under the Agreement.

If Customer does not object to a new subprocessor's engagement within fifteen (15) business days of notice issuance from Zoom, that new subprocessor shall be deemed accepted.

5.5 Zoom shall ensure that Authorized Subprocessors have executed confidentiality agreements that prevent them from unauthorized Processing of Customer Personal Data and Customer Content both during and after their engagement by Zoom.

5.6 Zoom shall, by way of contract or other legal act, impose on the Authorized Subprocessor data protection obligations consistent with the obligations set out in this Addendum and in accordance with GDPR requirements. The parties acknowledge and agree that notice periods shall be deemed equivalent regardless of disparate notification periods. If Personal Data are transferred to an Authorized Subprocessor in a third country that does not ensure an adequate level of protection according to the European Commission, the FDIPC, or UK Information Commissioner's Office, Zoom will ensure the transferred data are processed with the same GDPR transfer guarantees as agreed with Customer (such as Standard Contractual Clauses and BCRs). Zoom will also perform a case-by-case assessment if supplementary measures are required in cases of onward transfers to third countries to bring the level of protection of the transferred data up to the EU standard of essential equivalence.

5.7 Zoom shall be fully liable to Customer where that Authorized Subprocessor fails to fulfil its data protection obligations for the performance of that Authorized Subprocessor's obligations to the same extent that Zoom would itself be liable under this Addendum had it conducted such acts or omissions.

6. Security of Personal Data

6.1 Zoom may not update the Services in a way that would remove Customer's choice to apply end to end encryption to Meetings, introduce any functionality that would purposefully allow anyone not authorized by Customer to gain access to Customer encryption keys or Customer content, or remove the ability to store recordings locally.

6.2 Zoom certifies that it has not purposefully created any “back doors” or similar programming in the Services that could be used by third parties to access the system and/or Personal Data. Zoom has not purposefully created or

changed its business processes in a manner that facilitates such third-party access to Personal Data or systems. Zoom certifies there is no applicable law or government policy that requires Zoom as importer to create or maintain back doors or to facilitate access to Personal Data or systems or for the importer to be in possession of or to hand over the encryption key.

6.3 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Zoom shall maintain appropriate technical and organizational measures with regard to Customer Personal Data and to ensure a level of security appropriate to the risk, including, but not limited to, the **"Security Measures"** set out in Annex II to the Standard Contractual Clauses (attached here as EXHIBIT B). Customer acknowledges that the Security Measures are subject to technical progress and development and that Zoom may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

7. International Transfers of Personal Data

7.1 Zoom may not update the Services in a way that would remove Customer's ability to choose to store certain Personal Data at rest within the European Economic Area ("**EEA**").

7.2 Customer acknowledges and agrees that Zoom may transfer and process Customer Personal Data to and in the United States. Zoom may transfer Customer Personal Data to third countries (including those outside the EEA without an adequacy statement from the European Commission) to Affiliates, its professional advisors, or its Authorized Subprocessors, including when a Zoom End User knowingly connects to data processing operations supporting the Services from such locations (for example, when the End user travels outside of the territory of the EU). Zoom shall ensure that such transfers are made in compliance with Applicable Data Protection Law and this Addendum.

7.3 Any transfer of Customer's Personal Data made subject to this Addendum from member states of the European Union, the EEA, Switzerland or the United Kingdom to any country that does not ensure an adequate level of protection according to the European Commission, the FDIPC, or UK Information Commissioner's Office (as applicable), shall be undertaken through the Standard Contractual Clauses, in connection with which the parties agree to the following:

(a) **EU SCCs (Controller to Controller Transfers).** In relation to Personal Data that is protected by the EU GDPR and processed in accordance with Section 2.4 of this Addendum, the EU SCCs shall apply, completed as follows:

(i) Module One will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 11, the optional language will not apply;

(iv) in Clause 17, Option 1 will apply, and the New EU SCCs will be governed by Irish law;

(v) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vi) Annex I of the EU SCCs shall be deemed completed with the information set out in EXHIBIT A of this Addendum; and

(vii) Subject to Section 6.3 of this Addendum, Annex II of the EU SCCs shall be deemed completed with the information set out in EXHIBIT B to this Addendum.

(b) **EU SCCs (Controller to Processor/Processor to Processor Transfers).** In relation to Personal Data that is protected by the EU GDPR and processed in accordance with Sections 2.2 of this Addendum, the EU SCCs shall apply, completed as follows:

(i) Module Two or Module Three will apply (as applicable);

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 5.3 of this Addendum;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in EXHIBIT A to this Addendum; and

(viii) Subject to Section 6.3 of this Addendum, Annex II of the EU SCCs shall be deemed completed with the information set out in EXHIBIT B to this Addendum.

(c) **Transfers from the UK.** In relation to Personal Data that is protected by the UK GDPR, the UK Addendum will apply, completed as follows:

(i) The EU SCCs shall also apply to transfers of such Personal Data, subject to sub-Section (ii) below;

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above in Section 7.3 (a)-(b) of this Addendum, and the option "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Addendum.

(d) **Transfers from Switzerland.** In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply in accordance with Sections 7.3 (a)-(b), with the following modifications:

(i) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and

(iii) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDIPC and competent courts in Switzerland, unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA, in which event the Swiss SCCS shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in EXHIBIT A and EXHIBIT B to this Addendum.

7.4 It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this Addendum) the Standard Contractual Clauses shall prevail to the extent of such conflict.

7.5 Zoom may adopt a replacement data export mechanism (including any new version of or successor to the Standard Contractual Clauses or alternative mechanisms adopted pursuant to Applicable Data Protection Law) ("**Alternative Transfer Mechanism**"). So long as the Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to the territories to which Customer Personal Data is transferred on behalf of the Customer, Customer agrees to execute documents and take other reasonably necessary actions to give legal effect to such Alternative Transfer Mechanism.

7.6 Zoom will follow European Data Protection Board requirements and Applicable Data Protection Law requirements concerning the completion of a data transfer impact assessment ("**DTIA**").

8. Rights of Data Subjects

To the extent that Zoom is a Processor:

8.1 Zoom shall promptly notify Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under Applicable Data Protection Law. Zoom will advise the Data Subject to submit his or her request to Customer, and Customer will be responsible for responding to such request.

8.2 Zoom shall, taking into account the nature of the Processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the Data Subject's rights (regarding information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under Applicable Data Protection Law.

9. Disclosure of Personal Data

9.1 Zoom will not disclose or provide access to any Customer Personal Data except:

(a) as Customer directs;

(b) as described in this Addendum; or

(c) as required by law.

9.2 If a court, law enforcement authority or intelligence agency contacts Zoom with a demand for Customer Personal Data, Zoom will first assess if it is a legitimate order consistent with Zoom's Government Requests Guide. If so, Zoom will attempt to redirect this third party to request those data directly from Customer. If compelled to disclose or provide access to any Customer Personal Data to law enforcement, Zoom will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so, for example, through a so-called *gagging order.* If Zoom is prohibited by law from fulfilling its obligations under this Section 9.2, Zoom shall represent the reasonable interests of Customer. This is in all cases understood to mean:

(a) Zoom shall document a legal assessment of the extent to which: (i) Zoom is legally obliged to comply with the request or order; and (ii) Zoom is effectively prohibited from complying with its obligations in respect of Customer under this Addendum.

(b) Zoom shall only cooperate with the US issued request or order if legally obliged to do so and, where possible, Zoom shall judicially object to the request or order or the prohibition to inform Customer about this or to follow the instructions of Customer.

(c) Zoom shall not provide more Customer Personal Data than is strictly necessary for complying with the request or order.

(d) If Zoom becomes aware of a situation where it has reason to believe that the laws and practices in the third country of destination applicable to the processing of the Personal Data by Zoom, its Affiliates and Authorized Subprocessors, including any requirements to disclose Personal Data or measures authorizing access by public authorities, will prevent Zoom from fulfilling its obligations under this Addendum, Zoom will inform Customer without undue delay after Zoom becomes aware of such a situation.

(e) Zoom will publish a transparency report twice a year.

10. Compliance Auditing

10.1 Zoom will conduct third-party audits to attest to the ISO 27001 and SOC 2 Type II frameworks as follows:

(a) Zoom will conduct at least one audit annually. Starting in 2022, Zoom will audit the Security, Availability and Privacy Criteria in the SOC-2 audit.

(b) Audits will be performed according to the standards and rules of the regulatory or accreditation body for the applicable control standard or framework.

(c) Audits will be performed by qualified, independent, third-party security auditors at Zoom's selection and expense.

10.2 Each audit will result in the generation of an audit report ("**Zoom Audit Report**"), which Zoom will make available to Customer upon request. The Zoom Audit Report will be Zoom's Confidential Information. Zoom will promptly remediate issues raised in any Zoom Audit Report to the satisfaction of the auditor.

10.3 At its request and cost, Customer is entitled to have an audit carried out by a mutually agreed upon auditor to demonstrate that Zoom complies with the provisions of this Addendum and Clause 8.9 "*Documentation and compliance*" (EU SCCs) for the processing of Personal Data. Customer may exercise the right no more than once a year, except in respect of an additional audit following (i) a Zoom data breach or (ii) if specifically ordered by Customer's national Supervisory Authority.

10.4 Following receipt by Zoom of a request for an audit under this Section 10.4, Zoom and Customer will discuss and agree in advance on

(a) the identity of an independent and suitably qualified third-party auditor to conduct the audit;

(b) the reasonable start date and duration (not to exceed two weeks in respect of any on premise audits) of any such audit;

(c) the scope, process and normative framework of the audit, including: (i) the data processing outcomes, information, and control requirements to be in scope of the audit evidence requirements; and (ii) the nature and process for satisfactory audit evidence; and

(d) the security and confidentiality controls applicable to any such audit. All audits must be conducted in accordance with recognized international auditing standards.

10.5 Nothing in this Addendum will require Zoom to provide Personal Data of other Zoom customers or access to any Zoom systems or facilities that are not involved in the provision of the contracted Services.

11. Cooperation

Zoom shall provide Customer with all required assistance and cooperation in enforcing the obligations of the parties under Applicable Data Protection Law. To the extent that such assistance relates to the Processing of Customer Personal Data for the purpose of the performance of the Agreement, Zoom shall in any event provide Customer with such assistance relating to:

(a) The security of Customer Personal Data;

(b) Performing checks and audits;

(c) Performing Data Protection Impact Assessments ("**DPIA**");

(d) Prior consultation with the Supervisory Authority;

(e) Responding to requests from the Supervisory Authority or another government body;

(f) Responding to requests from Data Subjects;

(g) Reporting Customer Personal Data Breaches.

12. Security incidents and data breaches

12.1 In the event of a confirmed Personal Data Breach (at Zoom or at a subprocessor of Zoom), Zoom shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Zoom in its sole discretion deems necessary and reasonable to remediate such violation. In the event of such a Personal Data Breach, Zoom shall, taking into account the nature of the Processing and the information available to Zoom, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying (I) the relevant Supervisory Authority and/or (ii) Data Subjects affected by such Personal Data Breach without undue delay.

12.2 In the event of a large scale, as determined by Zoom, confirmed Personal Data Breach (with Zoom or an Authorized Subprocessor of Zoom), Customer allows Zoom to independently alert and consult the relevant Supervisory Authorities in order to better inform Customer what steps the Supervisory Authorities expect.

12.3 The obligations described in Sections 12.1 and 12.2 shall not apply if a Personal Data Breach results from the actions or omissions of Customer, except where required by Applicable Data Protection Law. Zoom's obligation to report or respond to a Personal Data Breach under Sections 12.1 and 12.2 will not be construed as an acknowledgement by Zoom of any fault or liability with respect to the Personal Data Breach.

13. Intentionally Omitted

14. General

14.1 This Addendum may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

14.2 Customer and Zoom acknowledge that the other party may disclose the Standard Contractual Clauses, this Addendum, and any privacy-related provisions in the Agreement to any Supervisory Authority upon request.

14.3 Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement, an Order Form, or any other documentation, with regard to the subject matter of this Addendum, this Addendum shall prevail to the extent of that conflict.

14.4 If there is a change in (i) Specific US State Data Protection Law, (ii) Applicable Data Protection Law, or (iii) a determination, decision, or order by a Supervisory Authority or competent court affecting this Addendum or the lawfulness of any Processing activities under this Addendum, then Zoom may propose supplements and modifications to this Addendum. If the Customer objects to the supplement or modification, then Customer must object to the supplement or modification within thirty (30) days or the right to object is waived. If Customer timely objects to the appropriateness of the supplement or modification, then the parties will work to resolve their differences, and if resolution cannot occur within thirty (30) days of Customer's notice of objection, then either party may terminate this Addendum and any affected portion(s) of the Agreement. All supplements and modifications will be in writing and signed by the parties, unless the terms of the Agreement provide otherwise.

14.5 The provisions of this Addendum are severable. If any phrase, clause or provision or Exhibit (including the Standard Contractual Clauses) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this Addendum or the remainder of the Exhibit, shall remain in full force and effect.

14.6 This Addendum shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

EXHIBIT A

Annex I: Description of the Processing/Transfer

Controller to Controller

(A) List of Parties:

Data Exporter	**Data Importer**
Name: **[•]**	Name: Zoom Communications, Inc.
Address: [counterpartyAddress_R3uB92J]	Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113, USA
Contact Person's Name, position and contact details: Name: Position: Email:	Contact Person's Name, position and contact details: Name: Deborah Fay Position: Data Protection Officer Address: Address: 55 Alma. 55 Almaden Blvd. Suite 600, San Jose, CA 95113, USA With a copy to e-mail: privacy@zoom.us
Activities relevant to the transfer: As described in Section (B) below	Activities relevant to the transfer: As described in Section (B) below
Role: Controller	Role: Controller

(B) Description of Transfer

Categories Data Subjects	
The personal data transferred concern the following categories of data subjects:	End Users
Purposes of the transfer(s)	
The transfer is made for the following purposes:	In accordance with Section 2.4 of this Addendum, Zoom may Process certain Customer Personal Data for its own Legitimate Business Purposes, as an independent Controller, solely when the Processing is strictly necessary and proportionate, and if the Processing is for one of the following exhaustive list of purposes: (a) Directly identifiable data (name, screen name, profile picture and email address and all Customer Personal Data directly connected to such directly identifiable data) may be Processed for: (i) billing, account, and Customer relationship management (marketing communications to procurement, sales, and other Customer personnel that requests such communication), and related Customer correspondence (mailings about for example necessary updates); (ii) complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data processed by Zoom as data Controller (for example website data), tax requirements, agreements and disputes; (iii) abuse detection, prevention, and protection (such as automatic scanning for matches with identifiers of known CSAM, virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and

	actions not permitted under Zoom´s Acceptable Use Guidelines; (b) Pseudonymized and/or aggregated data (Zoom will pseudonymise and/or aggregate as much as possible and pseudonymized and/or aggregated data will not be processed on a per-Customer level), for: (i) improving and optimizing the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of the Services, including zoom.us, explore.zoom.us, and support.zoom.us; (ii) internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including product strategy); and (iii) receiving and using Feedback for Zoom's overall service improvement.
Categories of Personal Data	
The personal data transferred concern the following categories of data:	**<u>Customer Content Data:</u>** **Zoom Account Profile Info:** Data associated with the End User account, profile picture, password, company name, and preferences. This includes: ● Zoom unique user ID, ● profile picture (optional) **<u>Diagnostic Data:</u>** **Meeting metadata:** Metrics about Service usage, including when and how meetings were conducted). This includes: ● event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID, and meeting ID) ● meeting session information, including frequency, average and actual duration, quantity, quality, network activity, and network connectivity ● number of meetings ● number of screen-sharing and non-screen-sharing sessions ● number of participants ● meeting host information ● host name ● meeting site URL ● meeting start/end Time ● join method ● performance, troubleshooting and diagnostics information **Telemetry data:** Data collected from locally installed software (applications and browser information about the deployment of Zoom Services and related systems environment / technical information. This includes: ● PC name ● microphone ● speaker ● camera ● domain ● hard disc ID ● network type ● operating system type and version ● client version ● MAC address

	● event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, ● user ID and meeting ID) ● service logs (information on systems events and states) **Other Service Generated Data:** ● spam identification ● push notifications ● Zoom persistent unique identifiers such as UUID or user ids that are combined with other data elements including: ● IP address ● Data center ● PC name ● Microphone ● Speaker ● Camera ● Domain ● Hard disc ID ● Network type ● Operating System Type and Version ● Client Version ● IP Addresses along the Network Path **<u>Support Data</u>:** ● problem description, post-meeting feedback
Frequency of the transfer	
Whether continuous or one-off.	The transfer of account information is one off, otherwise continuous when using the Service.
Special categories of personal data (if appropriate)	
The personal data transferred concern the following categories of sensitive data:	Not applicable if end to end encryption is enabled, and if End Users do not upload profile pictures revealing special categories of data.
Duration of processing:	In accordance with the retention period detailed below.
Nature and Subject Matter of the Processing:	Zoom will process Customer Personal Data for its own exhaustive list of Legitimate Business Purposes when strictly necessary and proportionate, in accordance with this Addendum.
Retention period (or, if not possible to determine, the criteria used to determine that period):	Zoom retains Customer Personal Data for as long as required for its own exhaustive list of Legitimate Business Purposes, in accordance with this Addendum. The criteria used to determine Zoom's retention periods include the following: ● The length of time of Zoom's relationship with Service users (for example, the duration of a Zoom account) ● Whether account owners modify or their users delete information through their accounts ● Whether Zoom has a legal obligation to keep the data (for example, certain laws require Zoom to keep records for a certain period of time) ● Whether retention is required by Zoom's legal position (such as in regard to the enforcement of agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

(C): Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative,

the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Personal Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioner's Office (the "**ICO**"). With respect to Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

Controller to Processor

(A) List of Parties:

Data Exporter	**Data Importer**
Name: **[•]**	Name: Zoom Communications, Inc.
Address: [counterpartyAddress_IgCfrvE]	Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113, USA
Contact Person's Name, position and contact details: Name: Position: Email:	Contact Person's Name, position and contact details: Name: Deborah Fay Position: Data Protection Officer Address: Address: 55 Alma. 55 Almaden Blvd. Suite 600, San Jose, CA 95113, USA With a copy to e-mail: privacy@zoom.us
Activities relevant to the transfer: As described in Section (B) below	Activities relevant to the transfer: As described in Section (B) below
Role: Controller	Role: Processor

(B) Description of Transfer

Categories Data Subjects	
The personal data transferred concern the following categories of data subjects:	Individuals about whom Personal Data is provided to Zoom via the Services by (or at the direction of) Customer or End Users, which may include without limitation Customer's or its Affiliates' employees, contractors, and End Users.
Purposes of the transfer(s)	
The transfer is made for the following purposes:	In accordance with Section 2.2 of the DPA, Zoom will only to the extent necessary and proportionate, Customer as Controller instructs Zoom to perform the following activities as Processor on behalf of Customer: ● Provide and update the Services as configured, and used by Customer and its users, (for example, through Customer's use of Zoom settings or administrator controls) including to make ongoing product improvements and provide personalised experiences and recommendations; ● Secure and real-time monitor the Services; ● Resolve issues, bugs, and errors; ● Provide Customer requested support, including applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymized; and ● Process Customer Personal Data as set out in the Agreement and this Annex I to the Standard Contractual Clauses (subject matter, nature, purpose, and duration of Personal Data Processing in the controller to processor capacity and any other documented instruction provided by Customer and acknowledged by Zoom as constituting instructions for purposes of this Addendum.

Categories of Personal Data	
The personal data transferred concern the following categories of data:	**<u>Customer Content Data:</u>** **Zoom Account Profile Info:** Data associated with the End User's Zoom account, profile picture, password, company name, and Customer's preferences. This includes: ● Zoom unique user ID, ● social media login (optional), ● profile picture (optional) and ● display name. **Customer authentication data:** This includes username and password unless Single Sign On (SSO) is used. **Meeting and webinar communication content.** This includes: ● video, audio, whiteboard, captions, and presentations ● in-meeting Questions & Answers, polls, and survey information ● closed captioning (Live Transcription) **Chat Messages.** 1:1 in-meeting and group chat messages that are not transferred to a permanent chat channel. **Customer Initiated cloud recordings**. This includes the following recordings if such recording is permitted by the Customer administrator controls and selected by a meeting host or participant: ● video recording of video, audio, whiteboard, captions, and presentations ● audio recording ● text file of all in meeting group chats ● audio transcript text file ● in-meeting Questions & Answers, polls, and survey information ● closed captioning transcripts **Meeting and webinar participant information.** This includes: ● registered participant name and contact details; and any data requested by Customer to be provided in conjunction with registration, email addresses ● status of participant (as host, as participants in a chat or as attendees) ● room names (if used) ● user categorizations ● tracking fields such as department or group ● scheduled time for a meeting ● topic names **Stored Chat Information.** This is data at rest (in storage) and includes: ● chat messages ● files exchanged via chat ● images exchanged via chat ● videos exchanged via chat ● chat channel title ● whiteboard annotations **Address book Information.** This includes contact information made available through Customer controlled integrations (e.g. Outlook) **Calendar Information.** This includes meeting schedules made available through Customer controlled integrations (e.g. Outlook, Google Calendar) **<u>Diagnostic Data:</u>**

	Meeting metadata: Metrics about Service usage, including when and how meetings were conducted). This category includes: ● event logs (including: action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID, and meeting ID) ● meeting session information, including frequency, average and actual duration, quantity, quality, network activity, and network connectivity ● number of meetings ● number of screen-sharing and non screen-sharing sessions ● number of participants ● meeting host information ● host name ● meeting site URL ● meeting start/end Time ● join method **Telemetry data:** Data collected from locally installed software (applications and browser information about the deployment of Zoom Services and related systems environment / technical information. This includes: ● PC name ● microphone ● speaker ● camera ● domain ● hard disc ID ● network type ● operating system type and version ● client version ● MAC address ● event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID and meeting ID) ● service logs (information on systems events and states) **Other Service Generated Data:** ● spam identification ● push notifications ● Zoom persistent unique identifiers such as UUID or user ids that are combined with other data elements including: ● IP address ● Data center ● PC name ● Microphone ● Speaker ● Camera ● Domain ● Hard disc ID ● Network type ● Operating System Type and Version ● Client Version ● IP Addresses along the Network Path **<u>Support Data:</u>** ● Contact name of support requestor, time, subject, problem description, post-meeting feedback (thumbs-up/down)

	● User supplied attachments including recordings, transcripts or screenshots, post-meeting feedback (open text provided with thumbs down)
Frequency of the transfer	
Whether continuous of one off.	Continuous
Special categories of personal data (if appropriate)	
The personal data transferred concern the following categories of sensitive data:	Special categories of data are not required to use the service. The Customer / data exporter can prevent the processing of these data by using end to end encryption in the Meetings and preventing End Users from uploading profile information that contains such special categories of data. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning an individual's health or sex life.
Duration of processing:	The term of the Agreement plus the period until Zoom deletes all Customer Personal Data processed on behalf of Customer in accordance with the Agreement.
Nature and Subject Matter of the Processing:	Zoom will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with this Addendum.
Retention period (or, if not possible to determine, the criteria used to determine that period):	Zoom retains Customer Personal Data for as long as required for its own exhaustive list of Legitimate Business Purposes, in accordance with this Addendum. The criteria used to determine Zoom's retention periods include the following: ● The length of time of Zoom's relationship with Service users (for example, the duration of a Zoom account) ● Whether account owners modify or their users delete information through their accounts ● Whether Zoom has a legal obligation to keep the data (for example, certain laws require Zoom to keep records for a certain period of time) ● Whether retention is required by Zoom's legal position (such as in regard to the enforcement of agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

(C) Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Personal Data to which the UK GDPR applies, the competent supervisory authority is ICO. With respect to Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT B

Technical and Organizational Security Measures

Zoom's technical and organizational security measures for Processing Customer Personal Data will meet the Minimum-Security Control Requirements set out in this EXHIBIT B ("**Security Measures**"). Customer recognizes that there may be multiple acceptable approaches to accomplish a particular minimum control requirement. Zoom must document in reasonable detail how a particular control meets the stated minimum control requirement. Zoom may revise the Security Measures from time to time. The term "should" in these Security Measures means that Zoom will use commercially reasonable efforts to accomplish the stated minimum control requirement and will document those efforts in reasonable detail, including the rationale, if any, for deviation.

As used in these Security Measures, (i) "including" and its derivatives mean "including but not limited to"; and (ii) any capitalized terms not defined in this EXHIBIT B shall have the same meaning as set forth in this Addendum.

1. Definitions

1.1 "**Systems**" means Zoom's production systems.

1.2 "**Assets**" means Zoom's production assets.

1.3 "**Facilities**" means Zoom's production facilities, whether owned or leased by Zoom (e.g., AWS, data centers).

2. Risk Management

2.1 Risk Assessment Program. The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.

2.2 Risk Assessment. A risk assessment must be performed annually to verify the implementation of controls that protect business operations and Customer Content.

3. Security Policy

3.1 A documented set of rules and procedures must regulate the Processing of information and associated services.

3.2 Security Policies and Exception Process. Security policies must be documented, reviewed, and approved, with management oversight, on a periodic basis, following industry best practices.

3.3 A risk-based exception management process must be in place for prioritization, approval, and remediation or risk acceptance of controls that have not been adopted or implemented.

3.4 Awareness and Education Program. Security policies and responsibilities must be communicated and socialized within the organization to Zoom personnel. Zoom personnel must receive security awareness training on an annual basis.

4. Organizational Security

4.1 A personnel security policy must be in place to establish organizational requirements to ensure proper training, competent performance, and an appropriate and accountable security organization.

4.2 Organization. Current organizational charts representing key management responsibilities for services provided must be maintained.

4.3 Background Checks. Where legally permissible, background checks (including criminal) must be performed on applicable Zoom personnel.

4.4 Confidentiality Agreements. Zoom personnel must be subject to written non-disclosure or confidentiality obligations.

5. Technology Asset Management

5.1 Controls must be in place to protect Zoom production assets, including mechanisms to maintain an accurate inventory of assets and handling standards for introduction and transfer, removal and disposal of assets.

5.2 Accountability. A process for maintaining an inventory of hardware and software assets and other information resources, such as databases and file structures, must be documented. Process for periodic asset inventory

reviews must be documented. Identification of unauthorized or unsupported hardware/software must be performed.

5.3 Asset Disposal or Reuse. If applicable, Zoom will use industry standards to wipe or carry out physical destruction as the minimum standard for disposing of assets. Zoom must have documented procedures for disposal or reuse of assets.

5.4 Procedures must be in place to remove data from production systems in which Customer's Personal Data are stored, processed, or transmitted.

6. Physical and Environmental

6.1 Controls must be in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.

6.2 Physical and Environmental Security Policy. Physical and environmental security plans must exist for facilities and scenarios involving access or storage of Customer's Personal Data. Additional physical and environmental controls must be required and enforced for applicable facilities, including servers and datacenter locations.

6.3 Physical Access. Physical access, to include visitor access to facilities, must be restricted and all access periodically reviewed.

6.4 Policies must be in place to ensure that information is accessed on a need-to-know basis.

6.5 Environmental Control. Facilities, including data and processing centers, must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection. Environmental control components must be monitored and periodically tested.

7. Communication and Connectivity

7.1 Zoom must implement controls over its communication network to safeguard data. Controls must include securing the production network and implementation of encryption, logging and monitoring, and disabling communications where no business need exists.

7.2 Network Identification. A production network diagram, to include production devices, must be kept current to facilitate analysis and incident response.

7.3 Data Flow Diagram. A current data flow diagram must depict data from origination to endpoint (including data which may be shared with subprocessors).

7.4 Data Storage. All of Customer's Personal Data, including Customer's Personal Data shared with subprocessors, must be stored and maintained in a manner that allows for its return or secure destruction upon request from Customer.

7.5 Firewalls. Firewalls must be used for the isolation of all environments, to include physical, virtual, network devices, production and non-production, and application/presentation layers. Firewall management must follow a process that includes restriction of administrative access, and that is documented, reviewed, and approved, with management oversight, on a periodic basis.

7.6 The production network must be either firewalled or physically isolated from the development and test environments. Multi-tier security architectures that segment application tiers (e.g., presentation layer, application and data) must be used.

7.7 Periodic network vulnerability scans must be performed, and any critical vulnerabilities identified must be remediated within a defined and reasonable timeframe.

7.8 Clock Synchronization. Production network devices must have internal clocks synchronized to reliable time sources.

7.9 Remote Access. The data flow in the remote connection must be encrypted and multi-factor authentication must be utilized during the login process.

7.10 Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (i.e., no split tunneling).

7.11 Subprocessors' remote access, if any, must adhere to the same controls and must have a valid business justification.

7.12 Wireless Access. Wireless access to the Zoom corporate network must be configured to require authentication and be encrypted.

8. Change Management

8.1 Changes to the production systems, production network, applications, data files structures, other system components, and physical/environmental changes must be monitored and controlled through a formal change control process. Changes must be reviewed, approved, and monitored during post implementation to ensure that expected changes and their desired result are accurate.

8.2 Change Policy and Procedure. A change management policy, including application, operating system, network infrastructure, and firewall changes must be documented, reviewed, and approved, with management oversight, on a periodic basis.

8.3 The change management policy must include clearly identified roles and responsibilities so as to support separation of duties (e.g., request, approve, implement). The approval process must include pre- and post-evaluation of change. Zoom posts service status and scheduled maintenance at https://status.zoom.us.

9. Operations

9.1 Documented operational procedures must ensure the correct and secure operation of Zoom's assets. Operational procedures must be documented and include monitoring of capacity, performance, service level agreements and key performance indicators.

10. Access Control

10.1 Authentication and authorization controls must be appropriately robust for the risk of the system, data, application, and platform; access rights must be granted based on the principle of least privilege and monitored to log access and security events, using tools that enable rapid analysis of user activities.

10.2 Logical Access Control Policy. Documented logical access policies and procedures must support role-based, "need-to-know" access (e.g., interdepartmental transfers, terminations) and ensure separation of duties during the approval and provisioning process. Each account provisioned must be uniquely identified. User access reviews must be conducted on a periodic basis.

10.3 Privileged Access. Management of privileged user accounts (e.g., those accounts that have the ability to override system controls), to include service accounts, must follow a documented process and be restricted. A periodic review and governance process must be maintained to ensure appropriate provisioning of privileged access.

10.4 Authentication and Authorization. A documented authentication and authorization policy must cover all applicable systems. That policy must include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized. Authentication credentials must be encrypted, including in transit to and from subprocessors' environments or when stored by subprocessors.

11. Data Integrity

11.1 Controls must ensure that any data stored, received, controlled, or otherwise accessed is accurate and reliable. Procedures must be in place to validate data integrity.

11.2 Data Transmission Controls. Processes, procedures, and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, to ensure data integrity during transmission and to validate that the data transmitted is the same as data received.

11.3 Data Transaction Controls. Controls must be in place to protect the integrity of data transactions at rest and in transit.

11.4 Encryption. Data must be protected and should be encrypted, both in transit and at rest, including when shared with subprocessors.

11.5 Data Policies. A policy must be in place to cover data classifications, encryption use, key and certificate lifecycle management, cryptographic algorithms and associated key lengths. This policy must be documented, reviewed, and approved with management oversight, on a periodic basis.

11.6 Encryption Uses. Customer Personal Data must be protected, and should be encrypted, while in transit and at rest. Customer Content must be protected, and should be encrypted when stored and while in transit over any network; authentication credentials must be encrypted at all times, in transit or in storage.

12. Incident Response

12.1 A documented plan and associated procedures, to include the responsibilities of Zoom personnel and identification of parties to be notified in case of an information security incident, must be in place.

12.2 Incident Response Process. The information security incident management program must be documented, tested, updated as needed, reviewed, and approved, with management oversight, on a periodic basis. The incident management policy and procedures must include prioritization, roles and responsibilities, procedures for escalation (internal) and notification, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.

13. Business Continuity and Disaster Recovery

13.1 Zoom must have formal documented recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations, and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable.

13.2 Business Recovery Plans. Comprehensive business resiliency plans addressing business interruptions of key resources supporting services, including those provided by subprocessors, must be documented, tested, reviewed, and approved, with management oversight, on a periodic basis. The business resiliency plan must have an acceptable alternative work location in place to ensure service level commitments are met.

13.3 Technology Recovery. Technology recovery plans to minimize service interruptions and ensure recovery of systems, infrastructure, databases, applications, etc. Must be documented, tested, reviewed, and approved with management oversight, on a periodic basis.

14. Back-ups

14.1 Zoom must have policies and procedures for back-ups of Customer's Personal Data. Backups must be protected using industry best practices.

14.2 Back-up and Redundancy Processes. Processes enabling full restoration of production systems, applications, and data must be documented, reviewed, and approved, with management oversight, on a periodic basis.

15. Third-Party Relationships

15.1 Subprocessors must be identified, assessed, managed, and monitored. Subprocessors that provide material services, or that support Zoom's provision of material services to Customers, must comply with control requirements no less stringent than those outlined in this document.

15.2 Selection and Oversight. Zoom must have a process to identify subprocessors providing services to Zoom; these subprocessors must be disclosed to Customer and approved to the extent required by this Agreement.

15.3 Lifecycle Management. Zoom must establish contracts with subprocessors providing material services; these contracts should incorporate security control requirements, including data protection controls and notification of security and privacy breaches must be included. Review processes must be in place to ensure subprocessors' fulfillment of contract terms and conditions.

16. Standard Builds

16.1 Production systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Zoom's security policies and standards.

16.2 Secure Configuration Availability. Standard security configurations must be established and security hardening demonstrated. Process documentation must be developed, maintained, and under revision control, with management oversight, on a periodic basis. Configurations must include security patches, vulnerability management, default passwords, registry settings, file directory rights and permissions.

16.3 System Patches. Security patch process and procedures, to include requirements for timely patch application, must be documented.

16.4 Operating System. Versions of operating systems in use must be supported and respective security baselines documented.

16.5 Desktop Controls. Systems must be configured to provide only essential capabilities. The ability to write to removable media must be limited to documented exceptions.

17. Application Security

17.1 Zoom must have an established software development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing, or implementing information systems. Zoom must ensure that web-based and mobile applications used to store, receive, send, control, or access Customer Personal Data are monitored, controlled, and protected.

17.2 Functional Requirements. Applications must implement controls that protect against known vulnerabilities and threats, including Open Web Application Security Project ("**OWASP**") Top 10 Risks and denial of service (DDOS) attacks.

17.3 Application layer controls must provide the ability to filter the source of malicious traffic.

17.4 Restrictions must also be placed on or in front of web server resources to limit denial of service (DoS) attacks.

17.5 Zoom must monitor uptime on a hosted web or mobile application.

17.6 Software Development Life Cycle. A Software Development Life Cycle (SDLC) methodology, including release management procedures, must be documented, reviewed, approved, and version-controlled, with management oversight, on a periodic basis. These must include activities that foster the development of secure software.

17.7 Testing and Remediation. Software executables related to client/server architecture that are involved in handling Customer Personal Data must undergo vulnerability assessments (both the client and server components) prior to release and on an on-going basis, either internally or using external experts, and any gaps identified must be remediated in a timely manner.

(c) Testing must be based on, at a minimum, the OWASP Top 10 risks (or the OWASP Mobile Top 10 risks, where applicable), or comparable replacement.

(d) Zoom must conduct penetration testing on an annual basis.

18. Vulnerability Monitoring

18.1 Zoom must continuously gather information and analyse vulnerabilities in light of existing and emerging threats and actual attacks. Processes must include vulnerability scans, anti-malware, Intrusion Detection Systems ("**IDS**")/Intrusion Prevention Systems (IPS), logging and security information and event management analysis and correlation.

18.2 Vulnerability Scanning and Issue Resolution. Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically and prior to system provisioning for production systems that process, store or transmit Customer Content.

18.3 Malware. In production, Zoom must employ tools to detect, log, and disposition malware.

18.4 Intrusion Detection/Advanced Threat Protection. Network and host-based intrusion detection/advanced threat protection must be deployed with events generated fed into centralized systems for analysis. These systems must accommodate routine updates and real-time alerting. IDS/advanced threat protection signatures must be kept up to date to respond to threats.

18.5 Logging and Event Correlation. Monitoring and logging must support the centralization of security events for analysis and correlation. Organizational responsibility for responding to events must be defined. Retention schedule for various logs must be defined and followed.

18.6 Zoom publishes a vulnerability disclosure policy at https://explore.zoom.us/en/trust/vulnerability-disclosure/ .

19. Cloud Technology

19.1 Adequate safeguards must ensure the confidentiality, integrity, and availability of Customer Personal Data stored, processed or transmitted using cloud technology (either as a cloud customer or cloud provider, to include subprocessors), using industry standards.

19.2 Audit Assurance and Compliance. The cloud environment in which data is stored, processed or transmitted must be compliant with relevant industry standards and regulatory restrictions.

19.3 Application and Interface Security. Threat modeling should be conducted throughout the software development lifecycle, including vulnerability assessments, including Static/Dynamic scanning and code review, to identify defects and complete remediations before hosting in cloud environments.

19.4 Business Continuity Management and Operational Resiliency. Business continuity plans to meet recovery time objectives (RTO) and recovery point objectives (RPO) must be in place.

19.5 Data Security and Information Lifecycle Management. Proper segmentation of data environments and segregation must be employed; segmentation/segregation must enable proper sanitization, per industry requirements.

19.6 Encryption and Key Management. All communications must be encrypted in-transit between environments.

19.7 Governance and Risk Management. Comprehensive risk assessment processes and centralized monitoring that enables incident response and forensic investigation must be used to ensure proper governance and oversight.

19.8 Identity and Access Management. Management of accounts, including accounts with privileged access, must prevent unauthorized access and mitigate the impacts thereof.

19.9 Infrastructure and Virtualization Security. Controls defending against cyberattacks, including the principle of least privilege, baseline management, intrusion detection, host/network-based firewalls, segmentation, isolation, perimeter security, access management, detailed data flow information, network, time, and a SIEM solution must be implemented.

19.10 Supply Chain Management, Transparency and Accountability. Zoom must be accountable for the confidentiality, availability and integrity of production data, to include data processed in cloud environments by subprocessors.

19.11 Threat and Vulnerability Management. Vulnerability scans (authenticated and unauthenticated) must be performed, both internally and externally, for production systems. Processes must be in place to ensure tracking and remediation.

20. Audits

20.1 At least annually, Zoom will conduct an independent third-party review of its security policies, standards, operations, and procedures related to the Services provided to Customer. Such review will be conducted in accordance with the AICPA's Statements on Standards for Attestation Engagements (SSAE), and Zoom will be issued a SOC 2 Type II report. Upon Customer's request, Zoom will provide Customer with a copy of the SOC 2 Type II report within thirty (30) days. If applicable, Zoom will provide a bridge letter to cover time frames not covered by the SOC 2 Type II audit period scope within 30 days, upon request by Customer. If exceptions are noted in the SOC 2 Type II audit, Zoom will document a plan to promptly address such exceptions and shall implement corrective measures within a reasonable and specific period. Upon Customer's reasonable request, Zoom will keep Customer informed of progress and completion of corrective measures.

20.2 Customer shall rely on the third-party audit SOC 2 Type II report for validation of proper information security practices and shall not have the right to audit, unless such right is granted under applicable law, except in the case of a Security Breach resulting in a material business impact to Customer. If Customer exercises the right to audit as a result of a Security Breach, such audit shall be within the scope of the Services. Customer will provide Zoom a minimum of thirty (30) days of notice prior to the audit. Zoom shall have the right to approve any third-party Customer may choose to conduct or be involved in the audit.

21. Specific Measures

Measure	Description
Measures of pseudonymisation and encryption of personal data	*Optional End-to-End Encryption for Meetings:* Users may choose to enable end-to-end encryption for Zoom meetings. This provides a high level of security since no third party — including Zoom — has access to the meeting's private keys. *Default Encryption:* The connection between a given device and Zoom is encrypted by default, using a mixture of TES 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used depend on whether a user uses the Zoom client, a web browser, a third-party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Zoom utilizes security measures to ensure the ongoing confidentiality, integrity, availability, and resilience of our processing systems and services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Zoom takes measures to facilitate the restoration of availability and access to our processing systems and services promptly in the event of a physical or technical incident.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Zoom implements a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the data we process.
Measures for user identification and authorisation	*Protections against unauthorised meeting participants*: Zoom has implemented numerous safeguards and controls to prohibit unauthorized participants from joining meetings: ● Eleven (11) digit unique meeting IDs ● Complex passwords ● Waiting rooms with the ability to automatically admit participants from your domain name or another selected domai ● Meeting lock feature that can prevent anyone from joining the meeting ● Ability to remove participants ● Authentication profiles that only allow entry to registered users, or restrict to specific email domains
Measures for the protection of data during transmission	*Optional End-to-End Encryption for Meetings*: Users may choose to enable end-to-end encryption for Zoom meetings. This provides a high level of security since no third party — including Zoom — has access to the meeting's private keys *Default Encryption*: The connection between a given device and Zoom is encrypted by default, using a mixture of TLS 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used depend on whether a user uses the Zoom client, a web browser, a third- party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper.
Measures for the protection of data during storage	*Cloud Recording Storage*: Cloud Recordings are processed and stored in Zoom's cloud after the meeting has ended; these recordings can be passcode-protected or available only to people in your organization. If a meeting host enables cloud recording and audio transcripts, both will be stored encrypted. *File transfer* storage: If a meeting host enables file transfer through in-meeting chat, those shared files will be stored encrypted and will

	be deleted within 31 days of the meeting. *Cloud recording access*: Recording access for a meeting is limited to the meeting host and account admin. The meeting/webinar host authorizes others to access the recording with options to share publicly, internal- only, add registration to view, enable/disable ability to download, and an option to protect the recording *Authentication*: Zoom offers a range of authentication methods such as SAML, Google Sign-in and Facebook Login, and/or Password based which can be individually enabled/disabled for an account. 2-*Factor* Authentication *("***2FA***"):* Admins can enable 2FA for your users, requiring them to set up and use 2FA to access the Zoom web portal.
Measures for ensuring physical security of locations at which personal data are processed	Controls are in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.
Measures for ensuring events logging	Zoom implements a standard requiring all systems to log relevant security access events.
Measures for ensuring system configuration, including default configuration	Zoom implements a standard specifying the minimum requirements for configuration management as it applies to Zoom's corporate and commercial environment.
Measures for internal IT and IT security governance and management	Zoom implements policies and standards governing internal IT and IT security governance and management.
Measures for certification/assurance of processes and products	Zoom implements a Security Audit and Accountability policy.
Measures for ensuring data minimisation	Zoom implements a privacy review in its software development lifecycle to align product development with the principle of data minimization.
Measures for ensuring data quality	Zoom implements a System and Information Integrity Policy.
Measures for ensuring limited data retention	We retain personal data for as long as required to engage in the uses described in our Privacy Statement, unless a longer retention period is required by applicable law. The criteria used to determine our retention periods include the following ● The length of time we have an ongoing customer relationship; ● Whether account owners modify or their users delete information through their accounts; • Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or • Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).
Measures for ensuring accountability	Zoom implements a Security Audit and Accountability policy.
Measures for allowing data portability and ensuring erasure	Zoom's paying customers can access their account data through their dashboard.