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	8435 3473 4432 015
Call-Off Contract reference	PS/24/139
Call-Off Contract title	Provision of Google Web Analytics Software
Call-Off Contract description	Provision of Google Web Analytics Software GA360
Start date	February 1st 2025
Expiry date	January 31st 2026
Call-Off Contract value	£70,680.00 (excluding VAT and any overages)
Charging method	BACS, annual upfront net 30 days
Purchase order number	DVLA Purchase Order will be submitted following receipt of signed Call off

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	**Redacted** **Redacted** @dvla.gov.uk Driver & Vehicle Licensing Agency (“DVLA”) Commercial Directorate C2 West DVLA Swansea SA6 7JL
To the Supplier	Merkle UK One Limited 10 Triton Street Regents Place London NW1 3BF United Kingdom Company number: 04238272
Together the ‘Parties’	

Principal contact details

For the Buyer:

Title: Commercial Specialist
Name: **REDACTED**
Email: **REDACTED**k@DVLA.gov.uk

For the Supplier:

Name **REDACTED**
Email: **REDACTED**@merkle.com
Phone: **REDACTED**

Call-Off Contract term

Start date	This Call-Off Contract Starts on **February 1st, 2025** and is valid for **12 months**.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). Subject to the below, the notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1). In the event of Ending without cause by the Buyer, the Buyer shall remain liable for the full 12 month Contract Value.

	Notwithstanding Buyer's right to early termination pursuant to this termination right and clause 18.1, the Supplier shall incur onwards costs until the Expiry Date specified in the Order Form. As such, in the event of such early termination, the Buyer shall remain liable to the Supplier for the full Call-off Contract Value (less any Losses the Supplier is reasonably and actually able to mitigate).
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **three months'** written notice before its expiry if: i. such extension is agreed by Google; and ii. with effect from commencement of such extension, in the event fees charged to the Supplier from the Services are increased, the Supplier shall be entitled to pass any such fee increase on to the Buyer.
	The extension period is subject to clauses 1.3 and 1.4 in Part B below, save that the above requirements for any such extension shall supersede clauses 1.3 and 1.4 in the event of conflict. 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.

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: Lot 2: Cloud software
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 1 and outlined below: 
Additional Services	N/A
Location	The Services will be delivered to DVLA, Swansea, SA6 7JL
Quality Standards	N/A
Technical Standards:	N/A
Service level agreement:	N/A
Onboarding	N/A

Offboarding	N/A

Collaboration agreement	N/A
Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £70,680.00 per year. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed £70,680.00 or 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 £70,680.00 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Buyer's responsibilities	The Buyer is responsible for payment of the call off contract charges.
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners: **Dentsu UK Limited** and the list of subprocessors in Schedule 10

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 annual up front in advance.
Invoice details	The Supplier will issue electronic invoices yearly. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to: **SSa.invoice@Ubusinessservices.co.uk**

Invoice information required	All invoices must include the designated purchase order number and details of services and products supplied.
Invoice frequency	Invoice will be sent to the Buyer annually
Call-Off Contract value	The total value for the initial 12 months of this Call-Off Contract is £70,680.00. This does not include VAT or any overages that may be incurred.
Call-Off Contract charges	The breakdown of the Charges is: £70,680.00 for a 12-month contract

Additional Buyer terms

Performance of the Service	N/A
Guarantee	N/A

Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	Terms essential for the provision of GA360 are added as a new Schedule 10
Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Personal Data and Data Subjects	See data processing terms in Schedule 10.
Intellectual Property	N/A
Social Value	N/A
Performance Indicators	Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.

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.

Signed	Supplier	Buyer
Name	**REDACTED**	**REDACTED**
Title	MD - Digital Analytics & Ad Tech	**REDACTED** Commercial Lead

Signature	REDACTED	REDACTED
Date	15/01/2025	15/01/2025

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

Buyer Benefits

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

G-Cloud 14 Buyer 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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
7 (Payment, VAT and Call-Off Contract charges)
8 (Recovery of sums due and right of set-off)
9 (Insurance)
10 (Confidentiality)
11 (Intellectual property rights)
12 (Protection of information)
13 (Buyer data)
19 (Consequences of suspension, ending and expiry)
24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 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

24.2 will not be taken into consideration.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

27.1 Except as specified in clause 29.8, a person who 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

[To be added in agreement between the Buyer and Supplier, and will be G-Cloud Services the Supplier is capable of providing through the Platform.]

As outlined in the pricing document for the G-Cloud 14 offering of **8435 3473 4432 015** and evidenced below, DVLA wish to utilise 200 million to 300 million events per month, with up to 5 support hours per month for a period of 12 months.

Events per month (tier)	Support hours per month	Effective monthly cost (excluding overages)	Annual cost (excluding overages)	Overage bands	Cost per overage
Up to 25 million	Up to 2 hours	£3,060.00	£36,720.0	25 million	£500.00
25 to 100 million	Up to 5 hours	£3,830.00	£45,960.0	25 million	£500.00
100 million to 200 million	Up to 5 hours	£4,770.00	£57,240.00	25 million	£500.00
200 million to 300 million	Up to 5 hours	£5,890.00	£70,680.00	25 million	£500.00

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. The detailed Charges breakdown for the provision of Services during the Term will include:

As outlined in the pricing document for the G-Cloud 14 offering of **8435 3473 4432 015** (embedded below), DVLA wish to utilise 200 million to 300 million events per month, with up to 5 support hours per month for a period of 12 months. This equates to **£70,680.00** for the 12-month period.

8435 3473 4432 015
- Pricing Document.oc

Schedule 3: Collaboration agreement NOT USED

This agreement is made on [enter date]

between:

[Buyer name] of [Buyer address] (the Buyer)

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address] together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

1.1.1 “Agreement” means this collaboration agreement, containing the Clauses and Schedules

1.1.2 “Call-Off Contract” means each contract that is let by the Buyer to one of the Collaboration Suppliers

1.1.3 “Contractor’s Confidential Information” has the meaning set out in the Call-Off Contracts

1.1.4 “Confidential Information” means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information

1.1.5 “Collaboration Activities” means the activities set out in this Agreement

1.1.6 “Buyer Confidential Information” has the meaning set out in the Call-Off Contract

1.1.7 “Default” means any breach of the obligations of any Collaboration Supplier or any Default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties 1.1.8 “Detailed Collaboration Plan” has the meaning given in clause 3.2

1.1.9 “Dispute Resolution Process” means the process described in clause 9

1.1.10 “Effective Date” means [insert date]

1.1.11 “Force Majeure Event” has the meaning given in clause 11.1.1

1.1.12 “Mediator” has the meaning given to it in clause 9.3.1

1.1.13 “Outline Collaboration Plan” has the meaning given to it in clause 3.1

1.1.14 “Term” has the meaning given to it in clause 2.1

1.1.15 "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent reenactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the "Term").

2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the "Outline Collaboration Plan").

3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the "Detailed Collaboration Plan"). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier's respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.

3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.

3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:

3.4.1 approve the Detailed Collaboration Plan
3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection

3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.

3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.

4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.

4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all cooperation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.

5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

6.2 Each Collaboration Supplier warrants that:

6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party

6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors

6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise

6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:

6.3.1 or becomes public knowledge other than by breach of this clause 6

6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party

6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure

6.3.4 independently developed without access to the Confidential Information

6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction

6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

7.1 Each Collaboration Supplier warrants and represents that:

7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good

industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£,000)].

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage
8.5.2 special loss or damage
8.5.3 consequential loss or damage
8.5.4 loss of profits (whether direct or indirect)
8.5.5 loss of turnover (whether direct or indirect)
8.5.6 loss of business opportunities (whether direct or indirect)
8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.

9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.

9.3 The process for mediation and consequential provisions for mediation are:

9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the President of the Law Society to appoint a Mediator

9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations

9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings

9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives

9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the Subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals):
Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position
: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position
: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position
: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position
: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position
: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position:
Date:

Collaboration Agreement Schedule 1: List of contracts

Collaboration supplier	**Name/reference of contract**	**Effective date of contract**

Collaboration Agreement Schedule 2 [**Insert Outline Collaboration Plan**]

Schedule 4: Alternative clauses NOT USED

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 USED

[A Guarantee should only be requested if the Supplier's financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary's requirements]

This deed of guarantee is made on [**insert date, month, year]** between:

(1) [**Insert the name of the Guarantor]** a company incorporated in England and Wales with number [insert company number] whose registered office is at [i**nsert details of the guarantor's registered office**] [or a company incorporated under the Laws of [**insert country**], registered in [**insert country**] with number [**insert number**] at [**insert place of registration**], whose principal office is at [**insert office details**]]('Guarantor'); in favour of
and

(2) The Buyer whose offices are [**insert Buyer's official address**]

('Beneficiary') **Whereas:**

The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.

It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn't needed then the section below and other references to the guarantee should be deleted.

Suggested headings are as follows:

Demands and notices
Representations and Warranties
Obligation to enter into a new Contract
Assignment
Third Party Rights
Governing Law
This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.

Guarantor company	[**Enter Company name**] **'Guarantor'**
Guarantor company address	[**Enter Company address**]
Account manager	[**Enter Account Manager name]**
	Address: [**Enter Account Manager address]**
	Phone: [**Enter Account Manager phone number]**
	Email: [**Enter Account Manager email**]
	Fax: [**Enter Account Manager fax** if applicable]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	Meaning
Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].
Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.
Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words ‘other’ and ‘otherwise’ are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

reference to a gender includes the other gender and the neuter

references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time

any phrase introduced by the words ‘including’, ‘includes’, ‘in particular’, ‘for example’ or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

fully perform or buy performance of the guaranteed obligations to the Buyer

as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[**Enter Address of the Guarantor in England and Wales**]

[**Enter Email address of the Guarantor**

representative] For the Attention of [**insert details**]

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

delivered by hand, at the time of delivery
posted, at 10am on the second Working Day after it was put into the post

sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
any amendment to or termination of the Call-Off Contract
any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee

it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person

if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor

the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

obtain judgement against the Supplier or the Guarantor or any third party in any court

make or file any claim in a bankruptcy or liquidation of the Supplier or any third party

take any action against the Supplier or the Guarantor or any third party

resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer's rights may be exercised as often as the Buyer deems expedient. Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation

has the capacity to sue or be sued in its own name

the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets

the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee

the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:

- the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgement, decree or permit to which the Guarantor is subject
- the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets
- all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgement.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor’s acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this
Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of

Guarantee by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers [**enter the Supplier name**] [or a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [**insert fax number**] from time to time to act as its authorised agent to receive notices, demands, Service of process

and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[**Insert name of the Guarantor**] acting by [**Insert names**]

Director

Director/Secretary

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

Buyer Guidance: Buyers should consider whether their Call-Off Contract contains adequate security measures in order to protect Personal Data in compliance with Annex B of the GDPR PPN 03/22

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: dataprotectionofficer@dft.gov.uk

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: **UKIDPO@dentsu.com**

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 for the purposes of Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of any Personal Data in respect of: • <u>Browsing Information</u> Any behaviour or action observed or recorded regarding an individual's interactions with or use of any of the Buyer's online resource including but not limited to website analytics, websites visited, time spent on websites, unique identifiers such as cookies or IP address. • <u>User account information</u> The Buyer's Google Analytic User's account information **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:*

	• *Business contact details of Supplier Personnel for which the Supplier is the Controller*, • *Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Framework Agreement) for which the Buyer is the Controller*,
Duration of the Processing	For 1 year from February 1st 2025-January 31st 2026
Nature and purposes of the Processing	Google service state that they collect the below data is the supply to the Analytics service which is consumed by DVLA. First-party cookies Google Analytics collects first-party cookies, data related to the device/browser, IP address (when collecting data, Google Analytics 4 does not log or store IP addresses), and on-site/app activities to measure and report statistics about user interactions on the websites and/or apps that use Google Analytics. Customers may customize cookies and the data collected with features like cookie settings, User-ID, Data Import, and Measurement Protocol. Learn more Google Analytics customers who have for instance, enabled the analytics.js or gtag.js collection method can control whether or not they use cookies to store a pseudonymous or random client identifier. If the customer decides to set a cookie, the information stored in the local first-party cookie is reduced to a random identifier (e.g., 12345.67890). For customers who use the Google Analytics for Apps SDK, we collect an App Instance Identifier, which is a number that is randomly generated when the user installs an app for the first time. Advertising identifiers Where customers use Google Analytics Advertising Features, Google advertising cookies are collected and used to enable features like Remarketing on the Google Display Network. These features are subject to the users' Ads Settings, the Policy requirements for Google Analytics Advertising Features and Google's EU User Consent policy, which requires customers to obtain consent for cookies where legally required—including consent for personalized ads. For more information about how Google uses advertising cookies, visit the Google Advertising Privacy FAQ. It is possible to implement Google Analytics without affecting normal data collection where Advertising features are disabled until consent is obtained (see Privacy Controls in Google

	Analytics), as well as prevent certain data from being used for advertising personalization purposes (See Advertising Personalization below). PII prohibition Our contracts prohibit customers from sending Personally Identifiable Information to Google Analytics. Customers should follow these Best Practices to ensure PII is not sent to Google Analytics. DVLA utilise the above service to provide insight in the actions and movements of user on the DVLA.gov website for use in enhancement of its services and customer facing interactions.
Type of Personal Data	**Online identifiers including:** • Cookies • Internet protocol addresses • Device identifiers • Device Client identifier • User's account information • User Login • User settings **SaaS User data, including:** • Name • Email Address • Telephone Number • Login • User settings • User change history
Categories of Data Subject	Depending on the nature of the Processor Services, these Data Subjects may include individuals: - To whom online advertising has been, or will be directed; - Who has visited specific websites or applications in respect of which the supplier provides the Processor Services; and/or - Who are customers or users of Buyer's products/services.
International transfers and legal gateway	**See Schedule 10 Data Processing Annex**

Plan for return and destruction of the data once the Processing is complete	The Personal Data shall remain the property of the Buyer and at the written direction of the Buyer, the Supplier shall securely transfer the Data to the Buyer or nominated third party and/or arrange for the secure destruction or deletion of each item of Personal Data (and any copies thereof) collected and processed in accordance with this Contract. DVLA – Any Personal Data will be deleted upon contract exit. See below for Googles data retention policy regarding their service – Data retention - Analytics Help (google.com)

Annex 2 - Joint Controller Agreement N/A

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

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

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 USED

Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Annual Revenue"	means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology: figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;

“Appropriate Authority” or “Appropriate Authorities”	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Cabinet Office Markets and Suppliers Team"	means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“Control”	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares,

	by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Corporate Change Event”	means: any change of Control of the Supplier or a Parent Undertaking of the Supplier; any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services; any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services; a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier; payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period; an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group; any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group; the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above

	occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;
"Corporate Change Event Grace Period"	means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;
"Corporate Resolvability Assessment (Structural Review)"	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;
"Critical National Infrastructure" or "CNI"	means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or significant impact on the national security, national defence, or the functioning of the UK;
"Critical Service Contract"	means the overall status of the Services provided under the Call-Off Contract as determined by the

	Buyer and specified in Paragraph 2 of this Schedule;
"CRP Information"	means the corporate resolution planning information, together, the: (a) Exposure Information (Contracts List); (b) Corporate Resolvability Assessment (Structural Review); and (c) Financial Information and Commentary
"Dependent Parent Undertaking"	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;
"FDE Group" **"Financial Distress Event"**	means the Supplier, Subcontractors the credit rating of an FDE Group entity dropping below the applicable Financial Metric; an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;

	there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity; an FDE Group entity committing a material breach of covenant to its lenders; a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute; any of the following: commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m; non-payment by an FDE Group entity of any financial indebtedness; any financial indebtedness of an FDE Group entity becoming due as a result of an event of default; the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity; in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and any two of the Financial Metrics for the Supplier not being met at the same time.
"Parent Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Public Sector Dependent Supplier"	means a supplier where that supplier, or that supplier's group has Annual Revenue of £50

	million or more of which over 50% is generated from UK Public Sector Business;
"Strategic Supplier"	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers;
"Subsidiary Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Supplier Group"	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"UK Public Sector Business"	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and
"UK Public Sector / CNI Contract Information"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;

Service Status and Supplier Status

This Call-Off Contract is not a Critical Service Contract.

[Guidance: A Critical Service Contract is a service contract which the Buyer has categorised as a Gold contract using the Cabinet Office Contract Tiering Tool available on the Knowledge Hub or which the Buyer, in consultation with the Cabinet Office Markets and Suppliers Team if appropriate, otherwise considers should be classed as a Critical Service Contract.]

The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is resolution.planning@cabinetoffice.gov.uk.

The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer's rights under this Schedule.

Provision of Corporate Resolution Planning Information

Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.

Subject to Paragraphs 3.6, 3.10 and 3.11:

where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and

except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.

The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

is full, comprehensive, accurate and up to date;

is split into three parts:

Exposure Information (Contracts List);

Corporate Resolvability Assessment (Structural Review);

Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector

Business and/or Critical National Infrastructure and the nature of those agreements; and

complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and

no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.

If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11) unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;

within 30 days of a Corporate Change Event unless

the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and the

Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

not required pursuant to Paragraph 3.10;

within 30 days of the date that:

the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or

none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or

not required pursuant to Paragraph 3.10.

Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

Aa3 or better from Moody's;

AA- or better from Standard and Poors;

AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

Termination Rights

The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP

Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

Confidentiality and usage of CRP Information

The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.

Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.

The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

redacting only those parts of the information which are subject to such obligations of confidentiality;

providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:

summarising the information;

grouping the information;

anonymising the information; and

presenting the information in general terms

The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST

The Supplier shall:

provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:

are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;

are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or

involve or could reasonably be considered to involve CNI;

provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

The Supplier shall:

provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;

ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and

provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information AND COMMENTARY

The Supplier shall:

provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and

ensure that the information is presented in a simple, effective and easily understood manner.

For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

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: GA360 Terms

Merkle UK One Limited - GA360 Terms

GA360 Terms set out herein are correct as of the Start Date. The parties agree and acknowledge that these Terms are based on pass-down Google terms. If Google updates the terms between Google and the Supplier (referred to as 'Company' in the GA360 Terms), to the extent that those terms relate to the services supplied under this Call-off Contract to the Buyer (referred to as 'Customer' in the GA360 Terms), the parties shall implement such change via the Variation process (such process not to be unreasonably refused or delayed by the Buyer) and the parties agree that such change shall be completed within not more than 30 days from the date Supplier supplies notification of such change to the Buyer.

ANNEX A - GMP RESELLER TERMS

Please check the GMP Reseller Terms (comprising the General Platform Terms, the GMP Advertising Service Specific Terms and the GA360 Service Specific Terms) regularly for updates as Google may amend the content contained within any embedded URLs. Any modifications to the GMP Reseller Terms will be available at the relevant URL or a different URL that Company provides from time to time pursuant to the terms of this Call-off Contract. Changes to the GMP Reseller Terms will not apply retroactively, save that changes to URL references and the content therein (including for example the Google Policies) will be effective immediately.

To the extent there is any conflict or inconsistency between any additional terms accepted within the user interface for the Services, an Order Form and the GMP Reseller Terms, the following order of precedence will apply: (1) any additional terms accepted within the user interface for the Services, (2) the Order Form, (3) as applicable to the Services, the GMP Advertising Service Specific Terms or the GA360 Service Specific Terms, and (4) the General Platform Terms.

Please note that the GMP Reseller Terms govern a number of different Services, including GMP Advertising Services and GA360 Services and subsequently certain GMP Reseller Terms may only apply to a particular Service.

GENERAL PLATFORM TERMS

1. DEFINTIONS & INTERPRETATION.

In the Agreement (defined below), the following terms are defined as:

1.1. "Ad(s)" means advertising content.
1.2. "Ad Specifications" means the features of an Ad that determine its compatibility with the criteria set by a Media Provider with respect to particular Media.
1.3. "Affiliate" means, with respect to the applicable entity, an entity that directly or indirectly controls, is controlled by or is under common control with such entity (and in the context of the Customer would include any Subsidiary).
1.4. "Agreement" means the Order Form together with the GMP Reseller Terms and, any additional terms accepted within the user interface.
1.5. "Anti-Bribery Laws" means all applicable commercial and public anti-bribery laws, including but not limited to the U.S. Foreign Corrupt Practices Act of 1977 and the UK Bribery Act 2010.
1.6. "Beta Feature" means any Service feature that is identified, including via the applicable Service user interface or via other communications to Customer, as "Beta", "Alpha", "Experimental", "Limited Release" or "Pre-Release" or that is otherwise identified as unsupported.
1.7. "Beta Test" means Customer's use of a Beta Feature(s) for the purpose of testing the usability and functionality of that Beta Feature(s). For purposes of clarification, (i) in no event will Customer be obligated to participate in any Beta Test, and (ii) Customer's use of a Beta Feature for purposes other

than testing the usability and functionality of that Beta Feature will not be deemed a Beta Test with respect to that Beta Feature.

1.8. "Campaign Manager Network" means an infrastructure within the Campaign Manager Service designed to allow Customer to segment its online advertising delivery and data collections.

1.9. "Campaign Manager UI" means the Campaign Manager Service user interface.

1.10. "Company" means the 'Company' detailed in the Order Form.

1.11. "Confidential Information" means information that one Party (or an Affiliate) discloses to the other Party under the Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances. It does not include information that is independently developed by the recipient, is lawfully given to the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient.

1.12. "CPM" means cost per 1,000 impressions.

1.13. "Customer" means the 'Customer' detailed in the Order Form.

1.14. "Customer Content" means any content served to End Users through the Target Properties that is not provided by or on behalf of Company pursuant to this Agreement (including the content of all Ads served via the Services).

1.15. "Customer Data" means the data derived from the Customer's use of the Services (including without limitation (i) with respect to Analytics 360, the data collected through use of an OSCI and then processed by Analytics 360; (ii) with respect to Optimize 360, Customer's creative content or code for creative content that Customer inputs into the Optimize 360 Service or has inputted on its behalf; and (iii) with respect to Tag Manager 360, data concerning the volume and frequency of Customer's code (e.g., HTML) or web beacons (e.g., pixel tag, clear GIF) served via a Tag Container).

1.16. "Customer Partner" means for Target Properties, (i) the owner (if not Customer) of a Target Property, (ii) the third party co-branding the Target Properties with Customer, or (iii) the third party for whom Customer is white labelling the Target Properties.

1.17. "Data Processing Terms" means the terms contained at the following URL: https://legal.dentsu.com/googlereseller#data-processing-terms.

1.18. "Data Protection Laws" means: (i) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and any implementing legislation (as amended); (ii) the GDPR; (iii) any other relevant and applicable data protection legislation or regulations; and (iv) Google's privacy policy as in force from time to time (available at https://www.google.com/privacypolicy.html or such other URL provided to Customer from time to time).

1.19. "Data Provider" means a provider of Third-Party Data. Subject to Customer's limited right to use Third Party Data under an Order Form, each Data Provider will retain all proprietary rights in and to its respective Third-Party Data.

1.20. "Display & Video 360 UI" means the Display & Video 360 Service user interface.

1.21. "Effective Date" has the meaning set out in the Order Form.

1.22. "End Users" means individual human end users of a Target Property.

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

1.24. "Exchange Spend" has the meaning given in the Order Form.

1.25. "GA360 Services" means any one or more of the following services selected in the Order Form: Analytics 360, Optimize 360, Surveys 360, Tag Manager 360.

1.26. "GA360 Service Specific Terms" means, for each of the GA360 Services, the additional terms and conditions that apply to such GA360 Services set out at this URL: https://legal.dentsu.com/googlereseller#ga360-service-specific-terms (see Annex B of this Schedule for the GA360 Service Specific Terms in place as of the Start Date.

1.27. "General Platform Terms" means these Google Marketing Platform terms and conditions (including Google Policies referred to herein) set out at this URL: https://legal.dentsu.com/googlereseller#generalplatform-terms.

1.28. "GDPR" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

1.29. "GMP Reseller Terms" means these 'General Platform Terms' and the 'GMP Advertising Service Specific Terms' and the 'GA360 Service Specific Terms' (as applicable).

1.30. “GMP Advertising Services” means any one or more of the following services selected in the Order Form: Display & Video 360 Service; Search Ads 360 Service; Campaign Manager Service; Nielsen Digital Ad Ratings Service.
1.31. “GMP Advertising Service Specific Terms” means, for each of the GMP Advertising Services, the additional terms and conditions that apply to such GMP Advertising Service set out at this URL: https://legal.dentsu.com/googlereseller#gmpads-service-specific-terms.
1.32. “Google” means Google Ireland Limited unless otherwise notified to Customer from time to time.
1.33. “Google Policies” means (i) the Google Platforms Program Policies available at https://support.google.com/platformspolicy; (ii) the Google Ad Manager Partner Guidelines available at https://support.google.com/admanager/answer/9059370; (iii) the Google EU User Consent Policy available at https://www.google.com/about/company/user-consent-policy.html (“EU User Consent Policy”); and (iv) any other policy and implementation guidelines identified in an applicable Order Form or provided to Customer (in each case, as updated from time to time).
1.34. “Government Officials” includes any government employee; candidate for public office; and employee of government-owned or government–controlled companies, public international organisations, and political parties.
1.35. “Initial Term” has the meaning given in the Order Form.
1.36. “Intellectual Property Rights” means all copyrights, moral rights, patent rights, trademarks, rights in or relating to Confidential Information and any other intellectual property or similar rights (registered or unregistered) throughout the world.
1.37. “Media” means online advertising inventory made available for purchase to Customer via the Display & Video 360 Service.
1.38. “Media Provider” means an advertising exchange, network, web publisher or other provider of Media.
1.39. “Monthly Service Fees” for a Service are the Service Fees payable by Customer with respect to that Service in a certain month.
1.40. “Non-Exchange Spend” has the meaning given in the Order Form.
1.41. “Order Form” means an order form, schedule or other agreement that is subject to these GMP Reseller Terms and sets forth pricing and other terms with respect to a particular Service.
1.42. “Personal Data” has the meaning given to it in the GDPR.
1.43. “Personally Identifiable Information” means (in the Agreement and any policies incorporated by reference into the Agreement) information that could be used on its own to directly identify, contact or precisely locate an individual.
1.44. “Renewal Term” has the meaning given in the Order Form.
1.45. “Reseller Arrangement” means Company’s relationship with Google as described in Clause 11.10.
1.46. “Services” means the following Google Marketing Platform services: GA360 Services and/or GMP Advertising Services.
1.47. “Service Fees” means the fees for the Service(s), transactions, products and product / technical support services, and all other fees set out in the Order Form(s) or in an applicable user interface for a Service.
1.48. “Spend” means the sum of Customer’s Exchange Spend and Non-Exchange Spend as reported by the Display & Video 360 Service.
1.49. “Subcontractor” means a subcontractor, consultant, third-party service provider or agent engaged by the Customer in connection with its use of Services.
1.50. “Subsidiary” means any entity that is controlled by the Customer.
1.51. “Tag” means code (e.g., HTML) or a web beacon (e.g., pixel tag, clear GIF) that requests the delivery of an Ad or tracks an Ad impression or click.
1.52. “Tag Container” means the code delivered through Tag Manager 360, through which Customer may serve multiple code (e.g., HTML) or web beacons (e.g., pixel tag, clear GIF) on one or more Properties.
1.53. “Target Property” means a property on which an Ad is served via the Services (i.e., web sites, consent-based email publications, approved software applications or other properties as approved from time to time) and with respect to Analytics 360 and Optimize 360, means any of the properties which use

an OSCI to send data to Analytics 360 through Customer's account, and with respect to Tag Manager 360, any web page, application, or other property for which Customer requests a Tag Container. "**Target Properties**" shall be construed accordingly.

1.54. "Tax" or "Taxes" means (without limitation) all taxes, duties, levies, imposts, withholdings, social security contributions, sales, use, excise, value-added, goods and services, consumption, other similar taxes or duties, deductions or amounts in the nature of or in respect of taxation.

1.55. "Term" has the meaning given in the Order Form.

1.56. "Third-Party Data" means the cookie-level information of a third party that is made available to Customer via the Display & Video 360 Service to target its purchases of Media.

1.57. "Third Party Fees" has the meaning given in the Order Form.

1.58. "UK GDPR" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

1.59. "Year" means each 12 month period commencing on the 1st June and expiring on 31st May during the Term.

2. THE PARTIES' OBLIGATIONS; PROHIBITED ACTS.

2.1. Company will:

2.1.1. use reasonable endeavours to set up the Customer's Services account within one month of the date of signature of the Order Form;

2.1.2. make available the applicable Services described in the Order Form(s) entered into by Company and Customer in accordance with these GMP Reseller Terms;

2.1.3. provide Customer access to web-based training (including product updates and recommendations) and support (including troubleshooting and technical maintenance support) if and where available for any particular Service;

2.1.4. provide (i) reasonable support to the Customer in accordance with the Google recommendations referenced in the Order Form and to the extent applicable, (ii) additional technical and/or support services in accordance with the description set out in the Order Form;

2.1.5. use current industry-standard security measures in connection with the provision of Services;

2.1.6. promptly notify Customer of any breach of security resulting in unauthorised third party access to the Customer Data; and

2.1.7. provide the Services in compliance with all applicable privacy and export laws, rules, regulations and sanctions programs, as well as applicable Internet advertising industry guidelines (e.g., the self-regulatory principles/code of conduct of the Network Advertising Initiative, the Interactive Advertising Bureau and the Digital Advertising Alliance).

2.2. Customer will:

2.2.1. use the Services in compliance with all applicable Google Policies and at all times Customer will bear the burden of proof in establishing such compliance;

2.2.2. be solely responsible for all use of Services (including, as applicable to the Services described in the Order Form(s), trafficking Ads, implementing Tags, all inquiries relating to Ads, the content of all Ads, obtaining necessary rights and consents for using Customer Data and other content or information provided to Company and/or Google, and the acts and omissions of all its Affiliates, Customer Partners and Subcontractors). This Clause 2.2.2 will not be treated as limiting Company's obligations with respect to the provision of the Services under the Agreement;

2.2.3. contact the Company directly with respect to the Services and/or any technical and/or support services in connection with its use of the GMP Advertising Services, and will not communicate directly with Google in respect of the same, except as expressly set out in Clauses 2.3;

2.2.4. obtain all rights necessary to use, and necessary to permit Company and in turn Google, to use the Customer Data under the terms of the Agreement, including from Customer Partners, owners of Target Property owners (if not Customer) and End Users;

2.2.5. use the Services in compliance with all applicable privacy and export laws, rules, regulations and sanctions programs, as well as applicable Internet advertising industry guidelines (e.g., the self regulatory

principles/code of conduct of the Network Advertising Initiative, the Interactive Advertising Bureau and the Digital Advertising Alliance);

2.2.6. ensure that each Target Property utilising a Service (and advise its Customer Partners in writing that each of their web sites and Target Properties must) contain a conspicuous link to a privacy policy that:

2.2.6.1. discloses:

2.2.6.1.1. the usage of third-party technology;

2.2.6.1.2. the data collection and usage resulting from the Services; and

2.2.6.1.3. that third parties may be placing and reading cookies on End Users' browsers, or using web beacons to collect information in the course of advertising being served on the web sites;

2.2.6.2. includes information about End Users' options for cookie management;

2.2.6.3. complies with all applicable privacy laws, rules and regulations; and

2.2.6.4. use reasonable endeavours to ensure that an End User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the End User's device in connection with the Services where providing such information or obtaining such consent is required by law.

2.3. Customer:

2.3.1. acknowledges that Google may from time to time: (a) send customer satisfaction surveys to the Customer for the purpose of gauging satisfaction with Company's services; and (b) request that the Company produce case studies relating to the Customer;

2.3.2. hereby confirms its willingness to participate in any customer satisfaction survey and/or case study, and will provide Google (and its appointed agents and representatives) with all assistance reasonably requested by Google in relation to such customer satisfaction surveys and case studies (including those that Company is requested to prepare under the aforementioned Clause 2.3.1(b)); and

2.3.3. hereby consents to: (a) Google contacting the Customer directly for the purposes set out in Clause 2.3.1; and (b) Google contacting the Customer directly to discuss the Customer's participation in any case studies; and (c) Company and Google's use of any such case studies as part of their respective marketing activities.

2.4. Customer will not, and will not assist or knowingly permit any third party to:

2.4.1. use the Services to process Personally Identifiable Information;

2.4.2. pass information to Company or Google that could be used or recognised as Personally Identifiable Information;

2.4.3. misappropriate, misuse or abuse any part of a Service;

2.4.4. modify, disassemble, decompile, reverse engineer, copy, reproduce or create derivative works from or in respect to any part of a Service (except to the extent that such prohibition is not permitted by law);

2.4.5. damage or tamper with any part of a Service;

2.4.6. knowingly breach any Service security measure;

2.4.7. remove or restrict Company's access to the Google Marketing Platform during the Term; or

2.4.8. provide any Ad that (i) when viewed or clicked on by an End User's computer, causes such End User's computer to download any software application, or (ii) is illegal.

3. PAYMENTS.

3.1. Customer will be solely responsible and liable for the payment of the Service Fees and all other applicable fees and costs incurred in connection with the Services.

3.2. For each applicable Service, Company will invoice (or send a statement of financial activity to) Customer for Monthly Service Fees in the month following the calendar month in which the Service Fees are incurred (unless there is an unforeseen circumstance where billing may be delayed) and all other Service Fees in accordance with the terms set out in the applicable Order Form. Customer will pay Company the Service Fees and all other amounts invoiced pursuant to Clause 3.1 (save for those disputed in good faith) within 30 days of the date of the invoice ("Payment Due Date"), in the currency and at the

exchange rate (if any) specified in the applicable Order Form and by electronic transfer to the account notified to it by Company or such other means expressly agreed to in writing by the Parties. Unless otherwise expressly agreed, Service Fees payable under an Order Form are additional to Service Fees payable under other Order Forms.

3.3. Upon prior notice to Customer, Company may, in its sole discretion if Company determines that there is any credit risk associated with Customer, require Customer to prepay Company reasonably anticipated or actual Service Fees under the applicable Order Form.

3.4. Company may charge interest at a rate of 8% per year above the base rate of Barclays Bank PLC, as updated from time to time, from the Payment Due Date until the date of actual payment, whether before or after judgment, on any amounts which are overdue (other than amounts disputed in good faith). Customer will pay reasonable expenses and legal fees Company incurs in connection with late payments not disputed in good faith.

3.5. Service Fees (and other applicable fees and costs) are exclusive of taxes. Notwithstanding any legal obligation on Customer to withhold any taxes from its payments to Company, Customer agrees to pay to Company a net amount equal to the full amount invoiced. Customer will pay all taxes and other government charges related to or arising from: (i) use of the Services; and (ii) Customer's obligations under the Agreement (in each case except for taxes on Company's net income).

3.6. Without prejudice to any other rights or remedies which Company has under the Agreement, if (a) Company determines there is any credit risk associated with Customer and Customer has not yet made or refuses to make prepayment pursuant to paragraph 3.3, or (b) Customer fails to pay Service Fees invoiced by Company (other than Service Fees disputed in good faith) within 15 days following the Payment Due Date, Company may in its sole discretion:

3.6.1. reduce Customer's access to the GMP Advertising Services to read only access; and/or

3.6.2. suspend each applicable Service (for which the Service Fees are overdue) after 10 days' notice to Customer; and/or

3.6.3. terminate the Agreement.

3.7. addition to other rights and remedies Company may have, Company may offset the Service Fees payable by Customer under the Agreement against any payment obligations to Customer that Company may incur under the Agreement or any other agreement between the Parties.

3.8. account and related billing and payment information which Customer provides to Company may be shared with third parties solely for the purposes of performing credit checks, effecting payment to Company or servicing Customer's account.

4. INTELLECTUAL PROPERTY.

4.1. Except to the extent expressly stated otherwise in the Agreement, neither Party will acquire any right, title or interest in any Intellectual Property Rights owned or licensed by the other Party.

5. CONFIDENTIALITY.

5.1. receiving Party will not disclose the Confidential Information of the disclosing Party, except to: Google, where Company is the receiving Party; Subcontractors, where the Customer is the receiving Party; Affiliates; employees; agents; and/or professional advisors of the receiving Party (in each case) who need to know it and who have agreed in writing (or in the case of professional advisors are otherwise bound) to keep it confidential.

5.2. receiving Party will ensure that those people and entities use the Confidential Information of the disclosing Party only to exercise rights and fulfil obligations under the Agreement, and that they keep it confidential.

5.3. receiving Party may also disclose Confidential Information when required by law after giving reasonable notice to the disclosing Party, if permitted by law.

5.4. For purposes of clarification, Customer Data and the terms and conditions of the Agreement are considered Confidential Information, and Customer Data shall, subject to Clause 3 (Customer Data) of the GMP Advertising Specific Terms and Clause 3 (Customer Data) GA360 Service Specific Terms be Confidential Information of Customer.

5.5. Notwithstanding this Clause 5 (Confidentiality), Clause 3 (Customer Data) of the GMP Advertising Specific Terms and Clause 3 (Customer Data) GA360 Service Specific Terms:

5.5.1. Company may provide Google with the following information: (a) details of the Customer; (b) details of the Service features adopted by the Customer; (c) a summary of the support it has provided to Customer, including average incident resolution times and the number of support escalations; and (d) Customer's renewal status (including anticipated likelihood of renewal and any potential renewal challenges);

5.5.2. With respect to the Display & Video 360 Service, Company and/or Google may share Customer's Spend data and Customer's identity with applicable Media Providers and Data Providers solely for reporting and billing purposes; and

5.5.3. With respect to Customer's participation in any Beta Test, Company may disclose to Google, and Google may use and disclose all results and feedback from the Beta Test, for any purpose, provided that neither Company nor Google will disclose such data, results or feedback to any other party in such a manner as would identify or reasonably be expected to identify Customer without Customer's prior written consent.

6. REPRESENTATIONS AND WARRANTIES.

6.1. Each Party warrants that it will use reasonable care and skill in complying with its obligations under the Agreement. Customer represents and warrants that it has all necessary rights and authority to (i) enter into each Order Form and bind Customer to the Agreement, (ii) perform its obligations hereunder and (iii) act on behalf of any Customer Partners.

6.2. No conditions, warranties or other terms apply to any Services or to any other goods or services supplied by Company under the Agreement unless expressly set out in the Agreement. Subject to Clause 6.1, no implied conditions, warranties or other terms apply (including any implied terms as to satisfactory quality, fitness for purpose or conformance with description).

6.3. Subject to Clause 6.1, Company will have no liability under the Agreement (including any indemnification obligations) arising out of or related to any use of Beta Features by Customer, its Affiliates, or its or the Customer Partners. Any use of Beta Features will be solely at Customer's own risk and may be subject to additional requirements as specified by Company. Company is not obligated to provide support for Beta Features and Company may, at its sole discretion, cease providing Beta Features as part of any Services.

7. INDEMNIFICATION.

7.1. Customer will indemnify Company and its Affiliates against:

7.1.1. any damages, losses, costs and expenses (including reasonable legal costs and expenses) and other liabilities suffered as a result of the Customer breaching any terms in this Agreement;

7.1.2. all damages and costs finally awarded against Company or its Affiliates in relation to a claim filed by a third party before a court or government tribunal:

7.1.2.1. that the creative, technology, data or other materials provided by Customer or any Affiliate of Customer to Company or Google or otherwise provided and utilised by Customer, any Affiliate of Customer or any Customer Partner in connection with the Services ("Customer Materials") infringes any trademark, trade secret, copyright, or U.S. patent of that third party; and/or

7.1.2.2. arising out of or related to: (a) any Customer Content or Target Property; (b) any use of, or access to, the Services, including Ads, by any Customer Partner; or (c) claims brought by any Customer Partner against Company or Google relating to the implementation or display of Ads on Customer Partner Target Properties or Google's and/or Company's provision of the Service(s) for such Customer Partner,

(each case arising under 7.1.2 being a “Third Party Claim”);

7.1.3. settlement costs in relation to that Third Party Claim;

7.1.4. reasonable legal fees and disbursements necessarily incurred by Company or any of its Affiliates in relation to that Third Party Claim; and

7.1.5. reasonable costs necessarily incurred by Company or any of its Affiliates in complying with Clause 7.2.

7.2. Company will:

7.2.1. notify the Customer of a Third Party Claim promptly after becoming aware of it;

7.2.2. provide the Customer with reasonable information, assistance and cooperation in responding to and, where applicable, defending that Third Party Claim; and

7.2.3. give the Customer sole control over the defence and settlement of that Third Party Claim subject to the Company’s right to join in the defence with non-controlling counsel of its choice and the Company’s rights under Clause 7.1.4.

7.3. If any of the Services become, or in Company or Google’s reasonable opinion are likely to become, the subject of an Intellectual Property Rights infringement claim, then Company will at the Company’s sole option and expense and upon notice to the Customer may: (a) procure the right to continue to provide the Services as contemplated by the Agreement; (b) modify the Services to render them non-infringing (if modification does not adversely affect use of the GMP Advertising Services); or (c) replace the Services with functionally equivalent, non-infringing services. If none of the foregoing options is commercially practicable, then each Party will have the right to terminate the Order Form.

8. LIMITATION OF LIABILITY.

8.1. Nothing in the Agreement will exclude or limit either Party’s liability:

8.1.1. for death or personal injury resulting from the negligence of either Party or their servants, agents or employees;

8.1.2. for fraud or fraudulent misrepresentation;

8.1.3. for payment of sums properly due and owing to the other in the course of normal performance of the Agreement; or

8.1.4. for any other liability that may not otherwise lawfully be excluded or limited.

8.2. Nothing in the Agreement will exclude or limit Customer’s liability under the indemnities given under the Agreement, including the indemnities given in Clause 7 (Indemnification) above.

8.3. Subject to Clauses 8.1, Company will not have any obligations or liability under or in connection with the Agreement (whether in contract, tort (including negligence) or otherwise) in relation to: (a) the content of Ads; or (b) any websites or content to which such Ads may link.

8.4. Subject to Clauses 8.1, 8.2 and 8.3, neither Party will be liable under or in connection with the Agreement (whether in contract, tort (including negligence) or otherwise) for any:

8.4.1. loss of profit;

8.4.2. loss of anticipated savings;

8.4.3. loss of business opportunity;

8.4.4. loss of or corruption of data (except for loss or corruption of Personal Data); or

8.4.5. indirect or consequential losses, suffered or incurred by the other Party,

(whether or not those losses were within the contemplation of the Parties at the date of the Agreement).

8.5. Subject to Clauses 8.1, 8.2, 8.3 and 8.4, Company’s aggregate liability (whether in contract, tort (including negligence) or otherwise) for all Claims (defined below) arising in each Year is limited to 100% of the Service Fees paid and payable under the Agreement in that Year.

For the purposes of this Clause 8.5, “Claims” means any claim, demand, proceeding, action or complaint of any nature or kind under or in connection with this Agreement.

9. TERM; TERMINATION; AND SUSPENSION.

9.1. The term of the Agreement is as set out in the applicable Order Form(s), subject to earlier termination in accordance with the Agreement.

9.2. Either Party may terminate the Agreement upon notice with immediate effect if the other Party is in material breach of the Agreement (which includes without limitation any breach by Customer of Clauses 2.2.1, 2.2.5, 2.4 or 3.2 of these General Platform Terms):

9.2.1. where the breach is incapable of remedy;

9.2.2. where the breach is capable of remedy and the Party in breach fails to remedy that breach within 30 days after receiving notice from the other Party; or

9.2.3. more than twice even if the previous breaches were remedied.

9.3. Termination. Company may terminate the Agreement immediately upon notice if child sexual abuse imagery is displayed on any Target Property.

9.4. If Company or Google is unable to provide a Service due to any changes in law or regulations, Company may terminate the Agreement and/or suspend the applicable Service upon notice to Customer.

9.5. Upon the expiration or termination of the Reseller Arrangement (whether in whole or in respect of certain Service(s)), Company may (in its sole discretion) either:

9.5.1. suspend and/or terminate the Agreement (either in whole or in respect of those Service(s)) upon notice to Customer; or

9.5.2. offer the Customer any or all of the following options (in Company's sole discretion):

9.5.2.1. consenting to the transfer of the Agreement by Company to Google (subject to Google agreeing to the same) pursuant to Clause 11.1; and/or

9.5.2.2. terminating the Agreement pursuant to Clause 9.5.1 and/or

9.5.2.3. terminating the Agreement pursuant to Clause 9.5.2 but continuing to receive the relevant Services directly from Google or its designee by executing the then-current applicable agreement(s) with Google or its designee; and/or

9.5.2.4. terminating the Agreement pursuant to Clause 9.5.1 but receiving third party services similar to the relevant Services from Company.

9.6. In the event the Customer reveals (either through conduct or notice) its intent to terminate the Agreement in accordance with its right set out herein, the Customer acknowledges and agrees that Company may notify Google of such intention to so terminate so that Google or Google's designee may, at its sole option, seek to enter into a direct agreement with the Customer with respect to the Services.

9.7. If Customer or a Customer Partner is in violation (or if Company reasonably suspects a violation or that such violation is reasonably likely to occur) of the GMP Reseller Terms (including without limitation any Anti-Bribery Laws, or the Data Processing Terms) then Company may immediately suspend or deactivate Customer's and/or Customer Partner's use of all or any part of the applicable Services.

10. EFFECT OF TERMINATION

10.1. Upon expiration or termination of the Agreement for any reason:

10.1.1. except as expressly stated otherwise, all rights and licences granted by each Party will cease immediately;

10.1.2. Company will cooperate in good faith to provide reasonable support and cooperation (which may include, at Customer's written request, the transfer of contact information, data and records necessary) to help ensure – to the extent within the reasonable control of the Company - a successful transition of the Services for the Customer. Such support and cooperation may be subject to additional fees and costs, such fees and costs to be agreed between the Parties at the time of the request; and

10.1.3. if requested, each Party will use commercially reasonable endeavours to promptly return to the other Party, or destroy and certify the destruction of, all Confidential Information (excluding Customer Data) disclosed to it by the other Party.

10.2. In the event Clause 9.5.2 applies:

10.2.1. Company will continue to provide the relevant Services to the Customer up until the earlier of the following circumstances (the "Transitional Period"): (i) the date the Customer indicates its preferred option (to the extent offered), and (ii) the date the Company is required by Google to cease reselling the applicable Service to the Customer;

10.2.2. Customer will continue to make payments to Company for Service Fees for the Services delivered during the Transitional Period; and

10.2.3. the terms of this Agreement will during the Transition Period continue in full force and effect during the Transition Period.

11. MISCELLANEOUS.

11.1. Anti-Bribery. In performance of its obligations under this Agreement, Customer: (a) will comply with AntiBribery Laws, which prohibit corrupt offers of anything of value, either directly or indirectly, to anyone, including Government Officials, to obtain or keep business or to secure any other improper commercial advantage; and (b) will not make any facilitation payments, which are payments to induce any official to perform routine functions they are otherwise obligated to perform. Any breach of this Clause 11.1 (AntiBribery) is deemed incapable of remedy. Customer will keep complete and accurate records relating to this Agreement. During the Term and for a period of one year afterwards, Company may audit Customer's relevant records to confirm Customer's compliance with this Agreement. Such auditor will only have access to those books and records of Customer that are reasonably necessary to confirm such compliance. Customer will make commercially reasonable and good faith efforts to comply with Company's anti-bribery due diligence process, including providing requested information.

11.2. Assignment. Company retains the right to transfer the Agreement to Google with Customer's consent. Customer may not assign any part of the Agreement without (i) the written consent of the Company; (ii) the written confirmation from the assignee that it has agreed in writing to be bound by the terms of the Agreement; and (iii) the assigning Party remaining liable for obligations under the Agreement if the assignee defaults on them. Any other attempt to assign is void.

11.3. Change of Control. If Customer experiences a change of control (for example, through a stock purchase or sale, merger, by operation of law, or other form of corporate transaction): (i) Customer will give written notice to Company within 30 days after the change of control; and (ii) the Company may immediately terminate the Agreement any time between the change of control and 30 days after it receives that written notice.

11.4. Conflicting Terms. If there is a conflict between the GMP Reseller Terms and a term of an Order Form, the term of the Order Form will govern. If there is any conflict between Clause 2.2 and the EU User Consent Policy, the EU User Consent Policy will apply in relation to End Users in the European Economic Area along with the UK.

11.5. Entire Agreement. Subject to Clause 8.1.2, the Agreement sets out all terms agreed between the Parties and supersedes all other agreements between the Parties relating to its subject matter. In entering into the Agreement neither Party has relied on, and neither Party will have any right or remedy based on, any statement, representation or warranty (whether made negligently or innocently), except those expressly set out in the Agreement.

11.6. Force Majeure. Neither Party will be liable for failure or delay in performance to the extent caused by circumstances beyond its reasonable control.

11.7. Governing Law. The Agreement is governed by English law and the Parties submit to the exclusive jurisdiction of the English courts in relation to any dispute (contractual or non-contractual) concerning the Agreement save that either Party may apply to any court for an injunction or other relief to protect its Intellectual Property Rights.

11.8. Notices. All notices of termination or breach must be in English, in writing and addressed to the other Party's Legal Department. The address for such notices to Company's Legal Department is UKLegalNotices@dentsu.com. All other notices (including notices of non-renewal) must be in English, in writing and addressed to the other Party's primary contact. Notice will be treated as given on receipt, as verified by written or automated receipt or by electronic log (as applicable).

11.9. No Agency. This Agreement does not create any agency, partnership, or joint venture between the Parties.

11.10. Reseller Arrangement. The Company has been appointed by Google (on a non-exclusive basis) to resell the Services. The Company: (i) is not acting as the agent, partner of, nor in joint-venture with Google; (ii) does not commit nor bind Google to this Agreement in any way; and (iii) does not give any promise, representation, warranty or guarantee on Google's behalf.

11.11. No Waiver. Neither Party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Agreement.

11.12. No Third-Party Beneficiaries. Save for in respect of Google, this Agreement does not confer any benefits on any third party unless expressly stated otherwise. The rights of the Parties to rescind or vary this Agreement are not subject to the consent of any other person.

11.13. Severability. If any term (or part of a term) of the Agreement is invalid, illegal or unenforceable, the rest of the Agreement will remain in effect.

11.14. Approvals. The Parties agree that whenever the Agreement calls for written request or written approval to be provided by either Party, unless otherwise expressly stated that email is not acceptable, such request or approval may be provided via email.

11.15. Equitable Relief. Nothing in the Agreement will limit a Party's ability to seek equitable relief.

11.16. Survival. Notwithstanding termination or expiration of the Agreement, any provisions of the Agreement that by their nature are intended to survive, will survive termination including, but not limited to: Clauses 3 (Payments), 4 (Intellectual Property), 5 (Confidentiality), 6.2 (Disclaimers), 6.3 (Beta Features), 7 (Indemnification), 8 (Limitation of Liability), 10 (Effect of Termination) and 11 (Miscellaneous).

1. **ANNEX B – GA360 SERVICE SPECIFIC TERMS** DEFINITIONS.

Capitalised terms not defined in these GA360 Service Specific Terms have the meanings given to them in the General Platform Terms section of the GMP Reseller Terms (found here: https://legal.dentsu.com/googlereseller#general-platform-terms).

In these GA360 Service Specific Terms:

1.1. "Enhanced Packet" has the meaning given in Clause 1.8.
1.2. "Event" means a base unit of measurement that is processed in the Analytics 360 Service through a GA4 Property, which may include but is not limited to a page view, transaction, call to the Google Analytics system by an OSCI, screen view, custom event or other interactions with GA4 Properties capable of supporting multiple data streams.
1.3. "GA-OEP Property" or "GA-OEP Properties" means the collection of settings and information associated with the same Property ID to which Hits or Events, as applicable, are sent from a Property or collection of Properties.
1.4. "Google Analytics 4 Property" or "GA4 Property" means an Analytics 360 Property (formerly known as an 'App + Web' property) that uses an OSCI to send Events to the GA360 Service through Customer's account.
1.5. "Google Analytics" means the standard 'Google Analytics' product made available to customers by Google for free.
1.6. "Google Standard Product Terms" means the applicable and then-standard (i) Google Analytics Terms of Service available at http://www.google.com/analytics/tos.html, (ii) Optimize Terms of Service available at http://g.co/optimizetos, and (iii) Google Tag Manager Terms of Service available at https://www.google.com/analytics/tag-manager/use-policy/, each as between Company and Customer.
1.7. "Google Tag Manager" means the standard 'Google Tag Manager' product made available to customers by Google for free.
1.8. "Hit" means a base unit of measurement that is sent to Analytics 360 for processing through a UA Property, which may include but is not limited to a page view, a transaction, or a call to the system by an OSCI.
1.9. "Mobile SDK" means a mobile operating system software development kit (together with any fixes, updates, and upgrades) made available to Customer by Company on Google's behalf so that developers may use in an application to send Hits or Events to the GA360 Services.
1.10. "OEP" means an "Optimize 360 Enabled Property", which is a GA-OEP Property that is enabled for linking to Optimize 360.
1.11. "Optimize" means the standard 'Optimize' product made available to customers by Google for free.
1.12. "Optimize Container" means the code delivered through Optimize 360, through which Customer may serve code required to deliver modified visitor experiences.
1.13. "OSCI" means an "Officially Supported Client Interface", which is a mechanism made available that can be used to send Hits and Events, as applicable, to Analytics 360.
1.14. "Platform Home" means the user interface in the Google Marketing Platform through which Customer can access certain platform-level functionality.
1.15. "Publisher" means a third party on whose web property or content Survey Questions may be placed.
1.16. "Report" means the resulting analysis shown at www.google.com/analytics (or any other URL Company may provide from time to time).
1.17. "Roll-Up Event" or "Roll-Up Hit" means an Event or Hit, respectively, that is additionally processed by a Roll-Up Property and stored therein.
1.18. "Roll-Up Property" means an Analytics 360 account configuration setting by which Event-or Hit-level data, as applicable, from one or more Properties is additionally processed by Analytics 360 without an OSCI and stored in accordance with such configuration.
1.19. "Sub-Property" means an Analytics 360 account configuration setting by which Event-level data from one GA4 Property is additionally processed by Analytics 360 without an OSCI and stored in accordance with such configuration.

1.20. "Sub-Property Event" means an Event that is additionally processed by a Sub-Property and stored therein.
1.21. "Survey Questions" means all questions submitted by Customer through Surveys 360.
1.22. "Survey Response Count" means the total number of completed surveys submitted by End Users in response to Survey Questions.
1.23. "Survey Response Data" means data submitted by End Users in response to Survey Questions.
1.24. “Universal Analytics Property” or “UA Property” means an Analytics 360 Property (also known as a ‘Classic’ property) that uses an OSCI to send Hits to the GA360 Service through Customer’s account.

2. GA360 SERVICES.

2.1. License Grant. Upon Customer’s execution of an Order Form indicating Customer’s acceptance of the GMP Reseller Terms, and on the condition Google approves the same, Company grants to Customer and Customer’s Subcontractors the non-exclusive right to access and use the GA360 Service, subject to the terms of the Agreement.

2.2. Customer is permitted to install, copy, and use the OSCIs (if Customer is purchasing Analytics 360) and GA360 Services solely on Customer’s Properties, subject to the terms and conditions of the Agreement.

2.3. If Customer’s GA360 Services account(s) (including accounts for any free versions of GA360 Service) is linked to a Google Marketing Platform organisation, certain data from Customer’s GA360 Service accounts and/or data related to or derived from Customer’s use of the Platform Home may be shared within the Google Marketing Platform organisation, made accessible to any entity or personnel with access to the Google Marketing Platform organisation, and will be subject to the applicable settings in the Platform Home. Notwithstanding Customer’s data sharing settings within any of the GA360 Service accounts linked to such Google Marketing Platform organisation, Company and Google support representatives may have access to the Google Marketing Platform organisation and its data for the purpose of troubleshooting or servicing the Google Marketing Platform organisation.

2.4. Company will use commercially reasonable efforts to ensure that the GA360 Service (other than Surveys 360) meets the service levels indicated at in Exhibit A (the “SLA”). In the event of an SLA violation, the Customer’s sole remedy shall be those specified in the SLA only.

2.5. Upon termination or expiration of the Order Form (as applicable):
2.5.1. each Property is subject to Google’s Downgrade Policies available at https://support.google.com/analytics/answer/9826983 (as modified from time to time) (“Downgrade Policies”) and may be subject to downgrade as outlined therein; and
2.5.2. the deletion terms in the Data Processing Terms will apply to the Customer Data to the extent applicable, and Company will procure Google otherwise:
2.5.2.1. delete Customer Data if requested by Customer through the GA360 Service features made available to Customer; or
2.5.2.2. render all Customer Data externally inaccessible within a reasonable time period after receiving a written request from Customer to do so; and
2.5.3. Company acknowledges that continued GA360 Service use is subject to the Google Standard Product Terms; and
2.5.4. Customer will not be permitted to export Customer Data processed in the performance of the GA360 Service except as the then-Standard Product Terms, as applicable, permits.

With respect to Surveys 360, sub-clause 2.5.2.2 will only apply to the extent such Customer Data has not been made public before termination or expiration of the Order Form for Surveys 360 by Customer.

2.6. Any Subsidiary of Customer may receive the GA360 Service(s) provided under the Order Form so long as such entity remains a Subsidiary of Customer and provided that Customer will be liable for the

acts and omissions of such Subsidiary to the extent any of such Subsidiary's acts or omissions, if performed by Customer, would constitute a breach of, or otherwise give rise to liability under the GMP Reseller Terms.

2.7. Data Processing Terms. The provision and use of the GA360 Services (excluding Surveys 360) is subject to the Data Processing Terms and the parties will comply with the Data Processing Terms with respect to such Services.

2.8. Save for in respect of Surveys 360, upon Customer's execution of an Order Form and resulting acceptance of the GMP Reseller Terms the Customer:
2.8.1. hereby enters into the Data Processing Terms; and
2.8.2. warrants that it has read and understood the Data Processing Terms and undertakes to comply with the Data Processing Terms.

3. CUSTOMER DATA.

3.1. As between Customer and Company, Customer will own all Customer Data and Company will take such actions reasonably necessary to ensure that Customer owns Customer Data provided that Customer authorises Company and in turn Google to use and disclose such Customer Data solely:
3.1.1. as aggregate Service statistics, which will not include Personally Identifiable Information or information that identifies or would reasonably be expected to identify Customer or any Target Properties;
3.1.2. to provide the GA360 Service and enforce its rights under this Agreement (it being understood and agreed that Customer's non-aggregated data will not be used or disclosed to any third party (except for Google or as otherwise expressly permitted by the Agreement) without Customer's written consent);
3.1.3. in accordance with the settings in Customer's account and the Platform Home, as applicable; and/or
3.1.4. if and as required by court order, law or governmental or regulatory agency (after, if permitted, giving reasonable notice to Customer and using reasonable endeavours to provide Customer with the opportunity to seek a protective order or the equivalent (at Customer's expense)).

3.2. Confidentiality. Notwithstanding Clause 5 (Confidentiality) of the General Platform Terms, and subject to these GA360 Service Specific Terms, Customer Data is Confidential Information of Customer.

4. ANALYTICS 360.

4.1. With respect to Analytics 360 the terms in this Clause 4 shall apply.

4.2. Customer will not, and will not allow any third party to, use data labelled as belonging to a third party in Analytics 360 for purposes other than generating, viewing, and downloading Reports.

4.3. Customer's use of Analytics 360 is subject to Google's Analytics 360 Policies available at www.google.com/analytics/policies (as modified from time to time) ("GA Policies").

4.4. If Customer links a Property to Firebase projects ("Firebase Linkage") as part of using Analytics 360, the following sub-clauses 4.4.1 and 4.4.2 will, in addition to the all other terms applicable terms set out in the Agreement, apply in respect of Customer's use of the Firebase Linkage:
4.4.1. certain data from Customer's Property, including Customer Data, may be made accessible within or to any other entity or personnel specified in the applicable Firebase settings; and
4.4.2. the Property may have certain Service settings modified by authorised personnel specified in the applicable Firebase settings (notwithstanding the settings Customer may have designated for that Property within Analytics 360).

In the event of a conflict between this Clause 4.4 and the remainder of this Agreement, the terms in this Clause 4.4 will govern and control solely with respect to Customer's use of the Firebase Linkage.

4.5. Unless otherwise agreed by Company in writing (in its sole discretion), Customer will not utilise its Analytics 360 account to process more than: (i) 20 billion Hits per month across all of Customer's Analytics 360 Properties; or (ii) 10 billion Hits per month for any individual Analytics 360 Property.

4.6. If an Analytics 360 Property is downgraded in accordance with the Order Form or at Customer's request, during the Term (and not in connection with any termination or expiration of the Order Form), the Downgrade Policies will apply, and any use of such downgraded property is subject to the Google Standard Product Terms for Google Analytics.

5. OPTIMIZE 360.

5.1. With respect to Optimize 360 the terms in this Clause 5 shall apply.

5.2. Notwithstanding any other provision in this Clause 5, Customer may only link GA-OEP Properties to Customer's Optimize 360 account if it has all necessary rights to such GA-OEP Properties and shared Analytics 360 data and has all necessary rights to perform such linking.

5.3. This Agreement governs Customer's use of Optimize 360 on Customer's OEPs only. Customer's use of the Optimize on free Optimize properties will be governed by the Google Standard Product Terms.

5.4. If Customer downgrades an OEP to Optimize, Company reserves the right for itself and on behalf of Google, to bill Customer in accordance with the rates listed on the Optimize 360 sales partner pricing page if experiments continue to run on such downgraded OEP.

6. SURVEYS 360.

6.1. With respect to Surveys 360 the terms in this Clause 6 shall apply.

6.2. Customer's use of Surveys 360 hereunder is subject to the Google Surveys Policies available at https://support.google.com/surveys/answer/2375134 (as modified from time to time, the "Google Surveys Policies").

6.3. Customer is solely responsible for the content of all Survey Questions. Customer acknowledges that Google owns all rights, title and interest in the decision tools, formulae, metrics, ratings, scores, tracking methodologies and data provided by Google or Company to generate the reports and/or provide Surveys 360, including data generated pursuant to Clause 3.1 (Customer Data) of these GA360 Service Specific Terms. In addition to the rights granted in Clause 3 of these GA360 Service Specific Terms, Customer grants to Company a perpetual, irrevocable, non-exclusive, worldwide, transferable, royalty free right to use, copy, modify, distribute, and display Customer Data not directly identifiable with Customer and derivatives thereof for the improvement, provision, and operation of Surveys 360 ("Licence"). Company is entitled to sub-licence the Licence to Google provided that Customer Data directly identifiable with Customer is not shared with any other parties without Customer's consent.

6.4. Notwithstanding anything to the contrary in the Agreement: Customer will indemnify Company, its Affiliates, directors, officers and employees against all liabilities, damages, losses, costs, fees (including legal fees), and expenses relating to any allegation or third-party legal proceeding to the extent arising from Customer's breach of: (i) Clause 6.3 of these GA360 Service Specific Terms; or (ii) the Google Surveys Policies. Subject to Clause 8.1 (Limitation of Liability) of the General Platform Terms, no limitations or exclusions of liability in the GMP Reseller Terms will apply to the indemnities in this paragraph.

7. TAG MANAGER 360.

7.1. With respect to Tag Manager 360 the terms in this Clause 7 shall apply.

7.2. Customer will not host the Tag Container on any domain other than the Tag Manager 360 domain without Company's prior written consent.

7.3. Customer represents and warrants that it has obtained all necessary rights to upload any non-Google tags and will comply with all terms and conditions relating to the use of all tags via Tag Manager 360.

7.4. Company is not liable for any claim or loss arising from or related to Customer's use of non-Google tags.

7.5. Customer will not configure its Tag Manager 360 account to request Tag Containers more than 20 billion times per month across all of a Customer's Tag Manager 360 Properties without Company's prior written consent.

EXHIBIT A

GA 360 Service Level Agreements

The following definitions shall apply for the purposes of this Exhibit A:

"Downtime" means the applicable definition of downtime set forth below for each SLA described below, in each case, excluding: (i) time resulting from technical malfunctions in the Mobile SDKs, in Customer's website's systems, or any other circumstances beyond Company's or Google's reasonable control (including, without limitation, Internet delays, network congestion and ISP malfunctions); and (ii) other than with respect to the UA 360 Collection SLA, time required for routine system maintenance (with notice to Customer, such as through in-product notifications) or Customer initiated account upgrades. Partial minutes or intermittent downtime for a period of less than one minute will not be counted towards Downtime. For purposes of the Collection SLAs, Downtime does not include client-side sampling.

"Uptime Percentage" means the total number of minutes in a calendar month minus the number of minutes of Downtime suffered in a calendar month, divided by the total number of minutes in a calendar month. For purposes of Analytics 360 and the GA 360 SLAs (as defined below), the 'total number of minutes in a calendar month are equal to the total number of minutes in a calendar month for which the applicable Property had an active Analytics 360 Order Form.

I. Analytics 360

Analytics 360 offers a different Service Level Agreement for each Property type available (either Universal Analytics (UA) or Google Analytics 4 (GA4)). If Customer has purchased Analytics 360 and is being billed according to GA4 Property Events under the relevant Order Form, the GA 360 SLA for GA4 Properties (detailed below) will apply. Otherwise if Customer has purchased Analytics 360 and is being billed according to Universal Analytics Property (formerly known as "Classic") Hits under the relevant Order Form, the UA 360 SLA (detailed below) will apply. In no event will Customer receive both the GA360 SLA and UA360 SLA under the same Order Form.

1. GA 360 SLA for GA4 Properties

Customer acknowledges that Google will use commercially reasonable efforts to ensure that the Analytics 360 Service meets the service levels indicated below for each GA4 Property (collectively, the "GA 360 SLAs"). If Google fails to meet the GA 360 SLAs in any calendar month, and if Customer meets its obligations under the GA 360 SLAs, Customer will be eligible to receive credit in accordance with the applicable credit percentage set forth below ("GA4 Credit") calculated against the Analytics 360 Monthly Service Fees paid by Customer for the calendar months during which Google failed to meet the applicable GA 360 SLAs.

In order to receive such GA4 Credit, Customer must notify Company of each impacted GA4 Property within 25 days from the time Customer becomes eligible to receive such GA4 Credit. Failure to comply with this requirement will forfeit Customer's right to such GA4 Credit. GA4Credit will be issued as a credit for the affected invoice (which Customer may apply to its following monthly invoice). The maximum GA4

Credit that Customer may be eligible for in the aggregate in any given calendar month is 25% of the Analytics 360 Monthly Service Fees for that month.

If Google fails to meet any of the GA 360 SLAs in any 3 consecutive months or in any 4 months in any 12consecutive month period, Customer will have a one-time right to terminate its Order Form upon prior written notice to Company, subject to such notice being received by Company within 25 days of the end of the month in which Customer becomes eligible for such right of termination. The remedies set forth in these GA 360 SLAs are Customer's sole and exclusive remedies for any failure to meet the GA 360 SLAs. Google will make an SLA determination in good faith based on its system logs, monitoring reports, configuration records, and other available information.

GA 360 SLA for GA4 Properties	Downtime	GA4 Credit % of Analytics 360 Monthly Service Fee	
Collection SLA: Analytics 360 Service collects Customer Data from GA4 Properties at an Uptime Percentage of at least 99.9%.	Periods during which time the collection component of the Analytics 360 Service is generally unavailable for a GA4 Property.	Uptime Percentage ≥96.0% but <99.9% ≥93.0% but <96.0% ≥90.0% but <93.0% <90.0%	GA4 Credit % 5% 10% 15% 25%
Reporting SLA: The reporting interface for GA4 Properties in the Analytics 360 Service is available for Customer's use at an Uptime Percentage of at least 99%. The Reporting SLA excludes the features set forth in the Reporting SLA Exceptions article available at https://support.google.com/analytics/answer/10999787 (as modified from time to time at Google's sole discretion) and does not apply to XL GA4 Properties.*	Periods during which time the Customer is unable to make a reporting request for a GA4 Property or otherwise log-in to the Analytics 360 Service interface for such GA4 Property.	Uptime Percentage ≥96.0% but <99.0% ≥93.0% but <96.0% ≥90.0% but <93.0% <90.0%	GA4 Credit % 5% 10% 15% 25%
Data Processing SLA: Except as set forth in the Data Processing SLA Exceptions article available at https://support.google.com/analytics/answer/10742670 (as modified from time to time at Google's sole discretion), the Analytics 360 Service processes collected Customer Data for each GA4 Property based on such Property's largest size classification* for the applicable calendar month as follows: (1) within 4 hours of receipt at an Uptime Percentage of at least 98% for Normal	Periods of processing delay during which time the Analytics 360 Service takes longer than the applicable timeframe for the corresponding GA4 Property size tier set forth in the Data Processing SLA to process collected Customer Data for such GA4 Property.	Uptime Percentage ≥96.0% but <98.0% ≥93.0% but <96.0% ≥90.0% but <93.0% <90.0%	GA4 Credit % 5% 10% 15% 25%

GA4 Properties; (2) within 48 hours of midnight (Pacific Time) at an Uptime Percentage of 98% of the time for Large GA4 Properties; and (3) within 7 days of midnight (Pacific Time) at an Uptime Percentage of 98% of the time for XL GA4 Properties.			

*For a given day, a Property is deemed (i) “Normal” if such Property has collected and processed fewer than 25 billion Events, (ii) “Large” if such Property has collected and processed 25 billion or more Events, and (iii) “XL” if such Property has collected and processed 250 billion or more Events, in each case, in the prior 31 day period (excluding the applicable given day (in the Property’s timezone)). Notwithstanding the foregoing, a Property may be deemed “XL” for a given day if such Property has collected and processed an average of 15 billion or more Events over the prior 7 day period (excluding the applicable given day (in the Property’s timezone)). For purposes of the Reporting SLA and Data Processing SLA under the GA 360 SLAs, the largest size classification given to GA4 Property under this paragraph in a calendar month period will determine the corresponding GA 360 SLA tier and/or availability for such Property over the same applicable calendar month.

The GA 360 SLAs apply solely to Customer Data collected directly through the then-current version(s) of OSCI (as defined in the GA360 Service Specific Terms, which, for the avoidance of doubt, excludes all deprecated features) and do not apply to any Customer Data collected, processed, or reported through the use of Integration Features or Universal Analytics Properties. For purposes of the GA 360 SLAs, ‘Integration Feature’ means any Analytics 360 Service feature that collects metrics by means other than through an OSCI, has an interface for displaying information collected via an OSCI that is separate from the Analytics 360 Service’s or exports metrics to other Google or third party products or services. Integration Features include (but are not limited to) any Analytics 360 Service features that collect metrics from or export metrics to other Google or third party products including Google Ads, AdSense, and BigQuery. Integration Features also include Firebase and apply to Customer’s use of, or data reported through, such service. The Reporting SLA does not apply to reporting on non-web based Google Analytics reporting UIs. The Collection SLA and Data Processing SLA only apply to the extent Customer sends data in accordance with the guidelines available at https://developers.google.com/analytics/ (as modified from time to time at Google’s sole discretion). Beta Features, including GA4 Properties participating in the Google Analytics Alpha Program, are excluded from the GA 360 SLAs.

2. UA 360 SLA for Universal Analytics Properties

Customer acknowledges that Google will use commercially reasonable efforts to ensure that the Analytics 360 Service meets the service levels indicated below for Universal Analytics Properties (collectively, the "UA 360 SLAs"). If Google fails to meet the UA 360 SLAs in any calendar month, and if Customer meets its obligations under the UA 360 SLAs, Customer will be eligible to receive credit in an amount equal to Analytics 360 Monthly Service Fees paid by Customer for the calendar months during which Google failed to meet the applicable UA 360 SLAs ("Analytics Credit").

In order to receive such Analytics Credit, Customer must notify Company within 25 days from the time Customer becomes eligible to receive such Analytics Credit. Failure to comply with this requirement will forfeit Customer's right to such Analytics Credit. Analytics Credit will be issued as a credit for the affected invoice (which Customer may apply to its following monthly invoice). For purposes of the Data Processing SLA, Company may, in lieu of providing the Analytics Credit pursuant to the terms of these SLAs, elect to re-process or restore applicable Customer Data, in which case Customer will no longer be eligible for such Analytics Credit. The maximum Analytics Credit that Customer may be eligible for in the aggregate in any given calendar month is 100% of Analytics 360 Monthly Service Fees.

If Google fails to meet any of the UA 360 SLAs in any 3 consecutive months or in any 4 months in any 12consecutive month period, Customer will have a one-time right to terminate its Order Form upon prior written notice to Company, subject to such notice being received by Company within 25 days of the end of the month in which Customer becomes eligible for such right of termination. The remedies set forth in

these UA 360 SLAs are Customer's sole and exclusive remedies for any failure to meet the UA 360 SLAs.

UA 360 SLAs for Universal Analytics Properties	Downtime
Collection SLA Analytics 360 Service collects Customer Data from Universal Analytics Properties at an Uptime Percentage of at least 99.9%.	Periods during which time the collection component of the Analytics 360 Service is generally unavailable to Google's customers.
Reporting SLA The reporting interface for Universal Analytics in the Analytics 360 Service is available for Company's use at an Uptime Percentage of least 99%.	Periods during which time the Customer is unable to log-in to the Analytics 360 Service interface for Universal Analytics.
Data Processing SLA Except as set forth in the Data Processing SLA Exceptions article available at https://support.google.com/analytics/answer/6223844?hl=en&ref_topic=2430414 (as modified from time to time at Google's sole discretion), the Analytics 360 Service processes collected Customer Data from Universal Analytics (1) within 4 hours of receipt at an Up-time Percentage of at least 98% for Universal Analytics Properties that receive fewer than or equal to 2 billion Hits per calendar month and (2) within 24 hours of midnight (Pacific Time) at an Uptime Percentage of 98% of the time for Universal Analytics Properties that receive more than 2 billion Hits per calendar month.	Periods of processing delay during which time the Analytics 360 Service takes longer than the applicable timeframe set forth in the Data Processing SLA to process collected Customer Data for Universal Analytics Properties.

The UA 360 SLAs apply solely to Customer Data collected directly through the then-current version(s) of OSCI (which, for the avoidance of doubt, excludes all deprecated features) and do not apply to any Customer Data collected, processed or reported through the use of Integration Features or GA4 Properties. For purposes of the UA 360 SLAs, “Integration Feature” means any Analytics 360 Service feature that collects metrics by means other than through an OSCI, has an interface for displaying information collected via an OSCI that is separate from the Analytics 360 Service's or exports metrics to other Google or third party products or services. Integration Features include (but are not limited to) any Analytics 360 Service features that collect metrics from or export metrics to other Google or third party products including Google Ads, AdSense, Firebase, and BigQuery. The Reporting SLA does not apply to reporting on non-web based Google Analytics reporting UIs. The Collection SLA and Data Processing SLA only apply to the extent Customer sends data in accordance with the guidelines available at https://developers.google.com/analytics/ (as modified from time to time at Google's sole discretion). Beta Features are excluded from the UA 360 SLAs.

II. Optimize 360

Customer acknowledges that Google will use commercially reasonable efforts to ensure that the Optimize 360 Service meets the service levels indicated below (collectively, the “Optimize 360 SLAs”). For clarity, the Optimize 360 SLAs do not apply during Downtime. If Google fails to meet the Optimize 360 SLAs in

any calendar month, and if Customer meets its obligations under the Optimize 360 SLAs, Customer will be eligible to receive credit in an amount equal to Optimize 360 Monthly Service Fees paid by Customer for the calendar months during which the Optimize 360 Service failed to meet the applicable Optimize 360 SLAs ("Optimize Credit").

In order to receive such Optimize Credit, Customer must notify Company within 25 days from the time Customer becomes eligible to receive such Optimize Credit. Failure to comply with this requirement will forfeit Customer's right to such Optimize Credit. Optimize Credit will be issued as a credit for the affected invoice (which Customer may apply to its following monthly invoice). The maximum Optimize Credit that Customer may be eligible for in the aggregate in any given calendar month is 100% of Monthly Service Fees.

If Google fails to meet any of the Optimize 360 SLAs in any 3 consecutive months or in any 4 months in any 12consecutive month period, Customer will have a one-time right to terminate its Order Form upon prior written notice to Company, subject to such notice being received by Company within 25 days of the end of the month in which Customer becomes eligible for such right of termination. The remedies set forth in these Optimize 360 SLAs are Customer's sole and exclusive remedies for any failure by Google to meet the Optimize 360 SLAs. For clarity, the Optimize 360 SLAs and beta features are Confidential Information under the GMP Reseller Terms.

Optimize 360 SLAs	Downtime
Optimize Container Delivery SLA: Customer's Optimize Containers, as most recently published by Customer, will be served to Properties configured to send Hits to an OEP and enabled under the Optimize 360 Service at the lesser of the following: (i) 99.99% of Optimize Container requests, as most recently published by Customer; or (ii) the total number of Optimize Container requests in any calendar month minus 500 Optimize Container requests.	Periods of Optimize 360 unavailability.

The Optimize Container Delivery SLA only applies (1) if Customer uses Optimize 360 in accordance with the terms of the Agreement, (2) when the Optimize Container is requested of an Optimize 360 server and (3) the total number of requests for all Optimize Containers across all Properties is no more than 20 billion per month, calculated on a calendar monthly basis. Beta Features are excluded from the Optimize 360 SLAs. The Optimize 360 SLAs are not offered under the Order Form (when Customer is billed on GA4 Property Events and the GA360 SLAs would apply) and are not available for Properties configured to send Events to an OEP unless explicitly agreed to in writing.

III. Tag Manager 360

Customer acknowledges that Google will use commercially reasonable efforts to ensure that the Tag Manager 360 Service meets the service levels indicated below (collectively, the "Tag Manager 360 SLAs"). For clarity, the Tag Manager 360 SLAs do not apply during Downtime. If Google fails to meet the SLAs in any calendar month, and if Customer meets its obligations under the Tag Manager 360 SLAs, Customer will be eligible to receive credit in an amount equal to Tag Manager 360 Monthly Service Fees paid by Customer for the calendar months during which the Tag Manager 360 Service failed to meet the applicable Tag Manager 360 SLAs ("Tag Manager Credit"). If Customer is receiving Tag Manager 360 for free, the "Tag Manager Credit" will be an amount equal to Company's standard wholesale Monthly Service Fee for up to 50,000,000 Tag Container requests per month as of the Tag Manager 360 Effective Date (e.g., $2,000 USD per month); provided however, such "Tag Manager Credit" amount will not exceed the total amount paid by Customer for all GA 360 products for the applicable calendar month(s) in which the Tag Manager 360 Service failed to meet the Tag Manager 360 SLAs.

In order to receive such Tag Manager Credit, Customer must notify Company within 25 days from the time Customer becomes eligible to receive such Tag Manager Credit. Failure to comply with this requirement will forfeit Customer's right to such Tag Manager Credit. Tag Manager Credit will be issued as a credit for the affected invoice (which Customer may apply to its following monthly invoice). The

maximum Tag Manager Credit that Customer may be eligible for in the aggregate in any given calendar month is 100% of Monthly Service Fees.

If Google fails to meet any of the Tag Manager 360 SLAs in any 3 consecutive months or in any 4 months in any 12-consecutive month period, Customer will have a one-time right to terminate its Order Form upon prior written notice to Company, subject to such notice being received by Company within 25 days of the end of the month in which Customer becomes eligible for such right of termination. The remedies set forth in these Tag Manager 360 SLAs are Customer's sole and exclusive remedies for any failure to meet the Tag Manager 360 SLAs.

Tag Manager 360 SLAs	Downtime
Tag Management Tag Container Delivery SLA: Customer's Tag Container requests, as most recently published by Customer, will be served to Properties enabled under the Tag Manager 360 Service at the lesser of the following: (i) 99.99% of Tag Container requests, as most recently published by Customer; or (ii) the total number of Tag Container requests in any calendar month minus 500 Tag Container requests.	Periods of Tag Manager 360 Service unavailability.
Tag Management Configuration SLA: The Tag Container configuration interface provided as part of the Tag Manager 360 Service is available for Customer's use in connection with the Tag Manager 360 Service at an Uptime Percentage of 99%.	Periods of Tag Manager 360 Service unavailability during which time the Customer is unable to log-in to the Tag Manager 360 front-end

The Tag Management Container Delivery SLA and Tag Management Configuration SLA only apply if Customer uses the Tag Manager Service 360 in accordance with this Agreement. The Tag Management Container Delivery SLA applies only when: (1) the Tag Container is requested of a Tag Manager 360 server; and (2) the total number of requests for all Tag Containers across all Properties is no more than 20 billion per month per Customer, calculated on a calendar monthly basis. Beta Features are excluded from the Tag Manager 360 SLAs.

ANNEX C – Data Processing Terms

Company and Customer have entered into the Agreement for the provision of the GA360 Services and/or GMP Advertising Services.

These "Data Processing Terms" (including the appendices) are entered into by Company and Customer and supplement the Agreement. These Data Processing Terms will be effective, and replace any previously applicable terms relating to their subject matter (including any data processing amendment or data processing addendum relating to the Services), from the later of 21 September 2022 and the Effective Date.

1. INTRODUCTION.

These Data Processing Terms reflect the Parties' agreement on the terms governing the processing of certain data in connection with the European Data Protection Legislation and certain Non-European Data Protection Legislation.

2. DEFINITIONS AND INTERPRETATION.

Capitalised terms not defined in these Data Processing Terms have the meanings given to them in the GMP Reseller Terms (found here: https://legal.dentsu.com/googlereseller).

In these Data Processing Terms:

2.1. "Additional Product" means a product, service or application provided by Company or Google or another third party that: (a) is not part of the Services; and (b) is accessible for use within the user interface of the Services or is otherwise integrated with the Services.
2.2. "Additional Terms for Non-European Data Protection Legislation" means the additional terms governing the processing of certain data in connection with certain Non-European Data Protection Legislation.
2.3. "Adequate Country" means:
(a) for data processed subject to the EU GDPR: the EEA, or a country or territory recognised as ensuring adequate data protection under the EU GDPR;
(b) for data processed subject to the UK GDPR: the UK, or a country or territory recognised as ensuring adequate data protection under the UK GDPR of the Data Protection Act 2018; and/or
(c) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) recognised as ensuring adequate data protection by the Swiss Federal Council under the Swiss FDPA, in each case, other than on the basis of an optional data protection framework.

2.4. "Alternative Transfer Solution" means a solution, other than Customer SCCs, that enables the lawful transfer of personal data to a third country in accordance with the European Data Protection Legislation, for example a data protection framework recognised as ensuring that participating local entities provide adequate protection.
2.5. "Customer Personal Data" means personal data that is processed by Company on behalf of Customer in the provision of the Services.
2.6. "Customer SCCs" means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Controller), and SCCs (Processor-to-Processor) as applicable.
2.7. "Data Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data on systems provided or managed by, or otherwise controlled by Company. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
2.8. "Data Subject Tool" means a tool (if any) made available by a Google Entity to data subjects that enables Google to respond directly and in a standardised manner to certain requests from data subjects in relation to Customer Personal Data (for example, online advertising settings or an opt-out browser plugin).

2.9. “EEA” means the European Economic Area.
2.10. “European Data Protection Legislation” means, as applicable: (a) the GDPR; and/or (b) the Swiss FDPA.
2.11. “European Laws” means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).
2.12. “Google Security Measures” has the meaning given in Section 7.1.2 (Google Security Measures).
2.13. “Google Subprocessors” has the meaning given in Section 10.1 (Consent to Subprocessor Engagement).
2.14. “Google Entity” means Google LLC (formerly known as Google Inc.), Google or any other Affiliate of Google LLC.
2.15. “Instructions” has the meaning given in Section 5.3 (Customer’s Instructions).
2.16. “New Subprocessor” has the meaning given in Section 10.1 (Consent to Subprocessor Engagement).
2.17. “Non-European Data Protection Legislation” means data protection or privacy laws in force outside the EEA, Switzerland and the UK.
2.18. “Notification Email Address” means the email address designated by Customer, and (a) set out in the Order Form or otherwise provided to Company in writing for the purpose of receiving certain notifications from Company relating to these Data Processing Terms and (b) provided to Google via the user interface of the Services or such other means provided by Google, to receive certain notifications from Google relating to these Data Processing Terms.
2.19. “Services” means the applicable services listed at privacy.google.com/businesses/adsservices.
2.20. “SCCs (Controller-to-Processor)” means the European Commission’s standard contractual clauses for the transfer of personal data to third countries pursuant to EU GDPR on a controller to processor basis, subject to the terms set out in Appendix 3 (Interpretation of Customer SCCs).
2.21. “SCCs (Processor-to-Controller)” means the European Commission’s standard contractual clauses for the transfer of personal data to third countries pursuant to EU GDPR on a processor to controller basis, subject to the terms set out in Appendix 3 (Interpretation of Customer SCCs).
2.22. “SCCs (Processor-to-Processor)” means the European Commission’s standard contractual clauses for the transfer of personal data to third countries pursuant to EU GDPR on a processor to processor basis, subject to the terms set out in Appendix 3 (Interpretation of Customer SCCs).
2.23. “Security Documentation” means any security certifications or documentation that Company may make available in respect of the Services.
2.24. “Security Measures” has the meaning given in Section 7.1.1 (Security Measures).
2.25. “Subprocessors” means third parties authorised under these Data Processing Terms to have logical access to and process Customer Personal Data in order to provide parts of the Services and any related technical support.
2.26. “Supervisory Authority” means, as applicable: (a) a “supervisory authority” as defined in the EU GDPR; and/or (b) the “Commissioner” as defined in the UK GDPR and/or the Swiss FDPA.
2.27. “Swiss FDPA” means the Federal Data Protection Act of 19 June 1992 (Switzerland).
2.28. “Term” means the period from the Effective Date until the end of Company’s provision of the Services under the Agreement.
2.29. The terms “controller”, “data subject”, “personal data”, “processing” and “processor” as used in these Data Processing Terms have the meanings given in the GDPR, and the terms “data importer” and “data exporter” have the meanings given in the applicable Customer SCCs.
2.30. The words “include” and “including” mean “including but not limited to” and any examples in these Data Processing Terms are illustrative and not the sole examples of a particular concept.
2.31. Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3. DURATION OF THESE DATA PROCESSING TERMS.

3.1. These Data Processing Terms will take effect on the Effective Date. Regardless of whether the Agreement has terminated or expired, these Data Processing Terms will remain in effect until, and automatically expire when Company and its Subprocessors delete all Customer Personal Data as described in these Data Processing Terms.

4. APPLICATION OF THESE DATA PROCESSING TERMS.

4.1. Application of European Data Protection Legislation. Section 5 (Processing of Data) to 12 (Contacting Company; Processing Records) (inclusive) will only apply to the extent that the European Data Protection Legislation applies to the processing of Customer Personal Data, including if:
4.1.1. the processing is in the context of the activities of an establishment of Customer in the EEA or the UK; and/or
4.1.2. Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services or the monitoring of their behaviour in the EEA or the UK.

4.2. Application to Services. These Data Processing Terms will apply to the Services to the extent set out in the Agreement.

4.3. Incorporation of Additional Terms for Non-European Data Protection Legislation. The parties will enter into Additional Terms for Non-European Data Protection Legislation to supplement these Data Processing Terms to reflect the application of the Non-European Data Protection Legislation.

5. PROCESSING OF DATA.

5.1. Processor and Controller Responsibilities. The parties acknowledge and agree that:
5.1.1. Appendix 1 describes the subject matter and details of the processing of Customer Personal Data;
5.1.2. Company is a processor of Customer Personal Data under the European Data Protection Legislation;
5.1.3. Customer is a controller or processor, as applicable, of Customer Personal Data under the European Data Protection Legislation; and
5.1.4. each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of Customer Personal Data.

5.2. Processor Customers. If Customer is a processor:
5.2.1. Customer warrants on an ongoing basis that the relevant controller has authorised: (i) the Instructions, (ii) Customer's appointment of Company as another processor, and (iii) Company's engagement of Subprocessors as described in Section 10 (Subprocessors);
5.2.2. Customer will immediately forward to the relevant controller any notice provided by Company under Sections 5.5 (Instruction Notifications), 7.2.1 (Incident Notification), 11 (Opportunity to Object to Subprocessor Changes) or that refers to any Customer SCCs; and
5.2.3. Customer may make available to the relevant controller any information made available by Company under Sections 9.6 (Data Centre Information) and 10.2 (Information about Subprocessors).

5.3. Customer's Instructions. By entering into these Data Processing Terms, Customer instructs Company to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and any related technical and/or support services; (b) as further specified via Customer's use of the Services (including in the settings and other functionality of the Services) and any related technical and/or support services; (c) as documented in the form of the Agreement, including these Data Processing Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Company as constituting instructions for purposes of these Data Processing Terms (collectively, the "Instructions").

5.4. Compliance with Instructions. Company will comply with the instructions unless prohibited by European Laws.

5.5. Instruction Notifications. Company will immediately notify Customer if, in Company's opinion: (a) European Laws prohibit Company from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Legislation; or (c) Company is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law. This Section 5.5 (Instruction Notifications) does not reduce either party's rights and obligations elsewhere in the Agreement.

5.6. Additional Products. If Customer uses any Additional Product, the Services may allow that Additional Product to access Customer Personal Data as required for the interoperation of the Additional Product with the Services. For clarity, these Data Processing Terms do not apply to the processing of personal data in connection with the provision of any Additional Product used by Customer, including personal data transmitted to or from that Additional Product.

6. DATA DELETION.

6.1. Deletion During Term - Services With Deletion Functionality. During the Term, if:
6.1.1. the functionality of the Services includes the option for Customer to delete Customer Personal Data;
6.1.2. Customer uses the Services to delete certain Customer Personal Data; and
6.1.3. the deleted Customer Personal Data cannot be recovered by Customer (for example, from the "trash"),
then Company will delete such Customer Personal Data from its systems as soon as reasonably practicable and within a maximum period of 180 days, unless European Laws require storage.

6.2. Deletion During Term - Services Without Deletion Functionality. During the Term, if the functionality of the Services does not include the option for Customer to delete Customer Personal Data, then Company will comply with:
6.2.1. any reasonable request from Customer to facilitate such deletion, insofar as this is possible taking into account the nature and functionality of the Services and unless European Laws require storage; and
6.2.2. in respect of processing undertaken by Subprocessors, the data retention practices described at policies.google.com/technologies/ads.

6.3. Company may charge a fee (based on reasonable costs incurred) for any data deletion under Section 6.2.1. Company will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such data deletion.

6.4. Deletion on Term Expiry. Customer instructs Company to delete all remaining Customer Personal Data (including existing copies) from its systems at the end of the Term in accordance with applicable law. Company will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Laws require storage.

7. DATA SECURITY.

7.1. Security Measures and Assistance.

7.1.1. Security Measures. Company will implement and maintain technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (the "Security Measures").

7.1.2. Google Security Measures. Appendix 2 describes the technical and organisational measures implemented by the Google Subprocessors ("Google Security Measures").

7.1.3. Access and Compliance. Company will: (a) authorise its employees, contractors and Subprocessors to access Customer Personal Data only as strictly necessary to comply with the Instructions; (b) take reasonable steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, and (c) ensure that all persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.4. Security Assistance. Company will (taking into account the nature of the processing of Customer Personal Data and the information available to Company) assist Customer in ensuring compliance with

Customer's (or where Customer is a processor, the relevant controller's) obligations in respect of security of personal data and personal data breaches, including Customer's (or where Customer is a processor, the relevant controller's) obligations under Articles 32 to 34 (inclusive) of the GDPR, by:
7.1.4.1. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Security Measures);
7.1.4.2. complying with the terms of Section 7.2 (Data Incidents); and
7.1.4.3. providing Customer with the Security Documentation in accordance with Section 7.4.1 (Reviews of Security Documentation) and the information contained in these Data Processing Terms.
7.1.5. Customer warrants and undertakes that it is satisfied that:
7.1.5.1. the Company and Subprocessors processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Company to process Customer Personal Data; and
7.1.5.2. the Company and Subprocessors have sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

7.2. Data Incidents.

7.2.1. Incident Notification. If Company becomes aware of a Data Incident, Company will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimise harm and secure Customer Personal Data.

7.2.2. Details of Data Incident. Notifications made under Section 7.2.1 (Incident Notification) will describe the nature of the Data Incident including the Customer resources impacted; the measures Company has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Company recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Company's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3. Delivery of Notification. Notification of any Data Incident will be delivered to the Notification Email Address or, at Company's discretion (including if Customer has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

7.2.4. Third Party Notifications. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident.

7.2.5. No Acknowledgement of Fault by Company. Notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Company of any fault or liability with respect to the Data Incident.

7.3. Customer's Security Responsibilities and Assessment.

7.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Company's obligations under Sections 7.1 (Security Measures and Assistance) and 7.2 (Data Incidents):
7.3.1.1. Customer is responsible for its use of the Services, including:
7.3.1.1.1. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data; and
7.3.1.1.2. securing the account authentication credentials, systems and devices Customer uses to access the Services; and
7.3.1.2. Company has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Company's and its Subprocessors' systems.

7.3.2. Customer's Security Assessment. Customer acknowledges and agrees that the Security Measures implemented and maintained by Company, and in turn its Subprocessors as set out in Section 7.1.1 (Security Measures), provide a level of security appropriate to the risk in respect of Customer Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals.

7.4. Reviews and Audits of Compliance.

7.4.1. Reviews of Security Documentation. To demonstrate compliance by Company with its obligations under these Data Processing Terms, Company will make the Security Documentation available for review by Customer.

7.4.2. Customer's Audit Rights.

7.4.2.1. Subject to reasonable written advance notice from the Customer the Company shall:
7.4.2.1.1. permit the Customer to conduct (and shall contribute to) audits and inspections of its systems and processes in relation to the processing of Customer Personal Data subject to the Customer ensuring:
7.4.2.1.1.1. that such audit or inspection is undertaken during normal business hours and with minimal disruption to the Company's business and the business of other clients of the Company; and
7.4.2.1.1.2. that all information obtained or generated by the Customer or its auditor(s) in connection with such audits and inspections is kept strictly confidential (save for disclosure to a regulatory authority or as otherwise required by Data Protection Laws);
7.4.2.1.2. give the Customer such information as is reasonably necessary to verify that the Company is in compliance with its obligations under Data Protection Laws; and
7.4.2.1.3. co-operate and assist the Customer with any data protection impact assessments and consultations with any regulatory authority that the Customer reasonably considers are relevant pursuant to Data Protection Laws in relation to the Customer Personal Data.

7.4.2.2. The cost of such audit, inspection, provision of information or data protection impact assessment shall be borne by the Customer.

7.4.2.3. The Customer may require the Company to conduct an audit or inspection of the Subprocessor's systems and processes in relation to the processing of Customer Personal Data. The cost of such an audit or inspection shall be borne by the Customer.

8. DATA SUBJECT RIGHTS.

8.1. Responses to Data Subject Requests. Company will notify Customer if it receives a request from or on behalf of a data subject of Customer Personal Data to exercise any of the rights given to data subjects by Data Protection Laws. Notwithstanding the aforementioned,
8.1.1. Google Subprocessors will respond directly to the data subject's request in accordance with the standard functionality of the Data Subject Tool (if the request is made via a Data Subject Tool); or
8.1.2. Customer or the Subprocessors will advise the data subject to submit their request to Customer (if the request if not made via a Data Subject Tool) and Customer
will be responsible for responding to such request.
8.2. Data Subject Request Assistance. Company will assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights, in all cases taking into account the nature of the processing of Customer Personal Data and, if applicable, Article 11 of the GDPR., by:
8.2.1. providing details of the functionality of the Services;
8.2.2. complying with the commitments set out in Section 8.1 (Responses to Data Subject Requests); and
8.2.3. if applicable to the Services, making available Data Subject Tools.

8.3. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for rectifying or deleting that data if required by the European Data Protection Legislation, including (where available) by using the functionality of the Services.

9. DATA TRANSFERS.

9.1. Data Storage and Processing Facilities. Subject to the remainder of this Section 9 (Data Transfers), Company may process Customer Personal Data in any country in which Company or any of its Subprocessors maintains facilities.

9.2. Restricted European Transfers. The parties acknowledge that the European Data Protection Legislation does not require the Customer SCCs or an Alternative Transfer Solution in order to process Customer Personal Data in or transfer it to an Adequate Country. If Customer Personal Data is transferred to any other country, and the European Data Protection Legislation applies to the transfers ("Restricted European Transfers"), then, and subject always to the terms in Appendix 1 (Subject Matter and Details of the Data Processing) dealing with Restricted European Transfers as between Company and Google and Google and Google Subprocessors, which will prevail in the event of conflict:
9.2.1. if Company adopts an Alternative Transfer Solution for any Restricted European Transfers, then the Company will ensure the Restricted European Transfer is made in accordance with that solution; and/or
9.2.2. if Company has not adopted an Alternative Transfer Solution for any Restricted European Transfers, then:
9.2.2.1. if Company's address is in an Adequate Country, the SCCs (Processor-to-Processor) will apply with respect to such Restricted European Transfers between Company and Subprocessors and,
9.2.2.2. in addition, if Company's address is not in an Adequate Country the SCCs (Controllerto-Processor) and/or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to Restricted European Transfers between Customer and Company.

9.4 Supplementary Measures and Information. Company will provide Customer with information relevant to Restricted Transfers, including information about supplementary measures protect Customer Personal Data, as described in Section 7.4.1 (Reviews of Security Documentation), Appendix 2 (Security Measures) and other materials concerning the nature of the Services and the processing of Customer Personal Data (for example, help centre articles).

9.5 Termination. If Customer concludes, based on its current or intended use of the Processor Services, that the Alternative Transfer Solution and/or Customer SCCs, as applicable, do not provide appropriate safeguards for Customer Personal Data, then Customer may immediately terminate the Agreement for convenience by notifying Company in writing.

9.6 Data Centre Information. Information about the locations of Google Subprocessor's data centres is available at www.google.com/about/datacenters/locations/.

10. SUBPROCESSORS.

10.1. Consent to Subprocessor Engagement. Customer specifically authorises the engagement of those entities listed at the URL specified in Section 10.2 as Subprocessors and further Subprocessors (together the "Google Subprocessors"). In addition, without prejudice to section 11 (Opportunity to Object to Subprocessor Changes) Customer generally authorises the engagement of any other third parties as Subprocessors and further Subprocessors (together the "New Subprocessors"). If the Restricted Transfers apply pursuant to Appendix 1, the above authorisations constitute Customer's prior written consent to the subcontracting by Company of the processing of Customer Personal Data in accordance with those terms.

10.2. Information about Subprocessors. Information about Subprocessors may be set out in the Order Form (Schedule 1 to this Annex C) and information about Google Subprocessors can otherwise be found at privacy.google.com/businesses/subprocessors.

10.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Company will ensure via a written contract that:
10.3.1. the Subprocessor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Data Processing Terms);
10.3.2. if the processing of Customer Personal Data is subject to the European Data Protection Legislation, the data protection obligations in these Data Processing Terms (as referred to in Article 28(3) of the GDPR, if applicable) are imposed on the Subprocessor; and
10.3.3. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11. OPPORTUNITY TO OBJECT TO SUBPROCESSOR CHANGES.

11.1. When any New Subprocessor is engaged during the Term, Company will inform the Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

11.2. Customer may object to any New Subprocessor by terminating for convenience immediately upon written notice to Company, on the condition that Customer provides such notice within 90 days of being informed of the engagement of the New Subprocessor as described in Section 11.1. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. CONTACTING COMPANY; PROCESSING RECORDS.

12.1. Contacting Company. Customer may contact Company in relation to the exercise of its rights under these Data Processing Terms via email to dpo@dentsu.com or via such other means as may be provided by Company from time to time. Company will provide prompt and reasonable assistance with Customer queries Company receives via such means, and that relate to the processing of Customer Personal Data under the Agreement.

12.2. Processing Records. Company will keep appropriate documentation of its processing activities as required by the GDPR. Customer acknowledges that Company is required under the GDPR to: (a) collect and maintain records of certain information, including: (i) the name and contact details of each processor and/or controller on behalf of which Company is acting and (if applicable) of such processor's or controller's local representative and data protection officer, and (ii) if applicable under the Customer SCCs, Customer's Supervisory Authority; and (b) make such information available to any Supervisory Authority. Accordingly, Customer will, where requested and as applicable to Customer, provide such information to Company upon request by Company and/or to Google Subprocessors upon request by Google Subprocessors via the user interface of the Services or via such other means as notified by Google Subprocessors, and will use such user interface or other means to ensure that all information provided is kept accurate and up-to-date.

12.3. Controller Requests. If Company receives a request or instruction via the methods described in Section 12.1 (or any other method) from a third party purporting to be a controller of Customer Personal Data, Company will advise the third party to contact Customer.

13. LIABILITY.

13.1. Liability Cap. The liability of the Parties under or in connection with these Data Processing Terms will be subject to the exclusions and limitations of liability in the Agreement.

13.2. Liability if the Customer SCCs Apply. If the Customer SCCs apply under Section 9 (Data Transfers), the total combined liability of Company and Google Subprocessors towards Customer under or in connection with the Agreement and the Customer SCCs combined will be subject to Section 13.1 (Liability Cap).

14. EFFECT OF THESE DATA PROCESSING TERMS.

14.1. Order of Precedence. If there is any conflict or inconsistency between the Customer SCCs, the Additional Terms for Non-European Data Protection Legislation, the remainder of these Data Processing Terms and/or the remainder of the Agreement, then the following order of precedence will apply:
14.1.1. the Customer SCCs (if applicable);
14.1.2. the Additional Terms for Non-European Data Protection Legislation (if applicable); 14.1.3. the remainder of these Data Processing Terms; and
14.1.4. the remainder of the Agreement.

14.2. Subject to the amendments in these Data Processing Terms, the Agreement remains in full force and effect.
14.3. No Modification of Customer SCCs. Nothing in the Agreement (including these Data Processing Terms) is intended to modify or contradict any Customer SCCs or prejudice the fundamental rights or freedoms of data subjects under the European Data Protection Legislation.
14.4. No Effect on Controller Terms. These Data Processing Terms will not affect any separate terms between Company and Customer reflecting a controller-controller relationship for a service other than the Services.
14.5. Legacy Customer SCCs. As of the later of 21 September 2022 and the Effective Date, these Data Processing Terms and the Customer SCCs will apply and will supersede and terminate any standard contractual clauses approved under the UK GDPR and the Data Protection Act 2018 and previously entered into by Customer and Company. This Section 14.5 (Legacy Customer SCCs) will not affect either party's rights, or any data subject's rights, that may have accrued under the Legacy Customer SCCs whilst they were in force.

15. CHANGES TO THESE DATA PROCESSING TERMS.

15.1. Changes to URLs. From time to time, Company may change any URL referenced in these Data Processing Terms and the content at any such URL, except that Company may only change the Customer SCCs in accordance with Sections 15.2.3 - 15.2.5 (Changes to Data Processing Terms) or to incorporate any new version of the Customer SCCs that may be adopted under the European Data Protection Legislation, in each case in a manner that does not affect the validity of the Customer SCCs under the European Data Protection Legislation.

15.2. Changes to Data Processing Terms. Company may change these Data Processing Terms if the change:
15.2.1. is expressly permitted by these Data Processing Terms, including as described in Section 15.1 (Changes to URLs);
15.2.2. reflects a change to the name of the Service, the addition or removal of a Service (or a feature of a Service) or a certain feature of the Service, has been recategorised as a controller service;
15.2.3. reflects a change in the name or form of a legal entity;
15.2.4. is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency, or reflect Company's adoption of an Alternative Transfer Solution; or
15.2.5. does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, (x) in the case of the Additional Terms for Non-European Data Protection Legislation, Company's rights to use or otherwise process the data in scope of the Additional Terms for Non-European Data Protection Legislation or (y) in the case of the remainder of these Data Processing Terms, Company's processing of Customer Personal Data, as described in Section 5.4 (Compliance with

Instructions); and (iii) otherwise have a material adverse impact on Customer's rights under these Data Processing Terms, as reasonably determined by Company.

15.3. Notification of Changes. If Company intends to change these Data Processing Terms under Section 15.2.4 or 15.2.5, Company will inform Customer without undue delay and always before the change will take effect by either: (a) sending an email to the Notification Email Address; or (b) alerting Customer via the user interface for the Services. If Customer objects to any such change, Customer may immediately terminate the Agreement for convenience by giving written notice to Company within 90 days of being informed of the change. This termination right is Customer's sole and exclusive remedy if Customer objects to a change to these Data Processing Terms under section 15.2.4 or 15.2.5.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Company's provision of the Services and any related technical support to Customer.

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Customer Personal Data by Company and its Subprocessors in accordance with these Data Processing Terms.

Nature and Purpose of the Processing

Company will process (including, as applicable to the Services and the Instructions), collecting, recording, organising, structuring, storing, altering, retrieving, using, disclosing, combining, erasing and destroying) Customer Personal Data for the purpose of providing the Services and any related technical support to Customer in accordance with these Data Processing Terms.

Types of Personal Data

Customer Personal Data may include the types of personal data described at privacy.google.com/businesses/adsservices.

Categories of Data Subjects

Customer Personal Data will concern the following categories of data subjects:

- data subjects about whom Google Subprocessors collect personal data in connection with the provision of the Services; and/or
- data subjects about whom personal data is transferred to Google Subprocessors in connection with the Services by, at the direction of, or on behalf of Customer.

Depending on the nature of the Services, these data subjects may include individuals: (a) to whom online advertising has been, or will be, directed; (b) who have visited specific websites or applications in respect of which Company provides the Services; and/or (c) who are customers or users of Customer's products or services.

Restricted European Transfers

Restricted European Transfers by Google. As between Company and Google and Google Subprocessors, if the processing of Customer Personal Data by Google involves any Restricted European Transfer, then:

(a) if Google adopts an Alternative Transfer Solution for any Restricted European Transfers, then such
Restricted European Transfers will be made in accordance with that solution; and/or
(b) if Google has not adopted or has informed Company that Google is no longer adopting an Alternative Transfer Solution for any Restricted Transfers, then:
a. if Google's address is in an Adequate Country:
i. the SCCs (Processor-to-Processor, Google Exporter) will apply with respect to Restricted Transfers from Google to Google Subprocessors; and
ii. in addition, if Company's address is not in an Adequate Country, the SCCs (Processor-to-Controller) will apply with respect to Restricted European Transfers between Google and Company (irrespective of the fact that Company may be a processor of Customer Personal Data); or

b. if Google's address is not in an Adequate Country the SCCs (Processor-to-Processor) will apply with respect to such Restricted European Transfers between Company and Google.

In respect of Restricted European Transfers by Google only, the following defined terms shall have the definitions below:

"SCCs (Controller-to-Processor)" means the terms at business.safety.google/adsprocessorterms/sccs/c2p.

"SCCs (Processor-to-Controller)" means the terms at business.safety.google/adsprocessorterms/sccs/p2c.

"SCCs (Processor-to-Processor)" means the terms at business.safety.google/adsprocessorterms/sccs/p2p.

"SCCs (Processor-to-Processor, Google Exporter)" means the terms at business.safety.google/adsprocessorterms/sccs/p2p-intra-group.

Appendix 2: Security Measures

This Appendix 2 sets out the Google Security Measures as at the Effective Date. These Google Security Measures may be updated or modified from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1) Data Centre & Network Security
a) Data Centres.

Infrastructure. Google maintains geographically distributed data centres. Google stores all production data in physically secure data centres.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimise the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data centre equipment is scheduled through a standard process according to documented procedures.

Power. The data centre electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data centre. Backup power is provided by various mechanisms such as uninterruptible power supply (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-oftolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data centre, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data centre at full capacity typically for a period of days.

Server Operating Systems. Google servers use hardened operating systems which are customised for the unique server needs of the business. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Business Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

Encryption Technologies. Google's security policies mandate encryption at rest for all user data, including personal data. Data is often encrypted at multiple levels in Google's production storage stack in data centres, including at the hardware level, without requiring any action by customers. Using multiple layers of encryption adds redundant data protection and allows Google to select the optimal approach based on application requirements. All personal data is encrypted at the storage level, generally using AES256.

Google uses common cryptographic libraries which incorporate Google's FIPS 140-2 validated module, to implement encryption consistently across the Processor Services.

b) Networks & Transmission.

Data Transmission. Data centres are typically connected via high-speed private links to provide secure and fast data transfer between data centres. Further, Google encrypts data transmitted between data centres. This is designed to prevent data from being read, copied, altered or removed without authorisation during electronic transport. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

i) Tightly controlling the size and make-up of Google's attack surface through preventative measures;

ii) Employing intelligent detection controls at data entry points; and

iii) Employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as TLS connection) available. Google servers support ephemeral elliptic curve Diffie Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimise the impact of a compromised key, or a cryptographic breakthrough.

2) Access and Site Controls
a) Site Controls.

On-site Data Centre Security Operation. Google's data centres maintain an on-site security operation responsible for all physical data centre security functions 24 hours a day, 7 days a week. The on-site security operations personnel monitor Closed Circuit TV ("CCTV") cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data centre regularly.

Data Centre Access Procedures. Google maintains formal access procedures for allowing physical access to the data centres. The data centres are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data centre are required to identify themselves as well as show proof of identity to on-site security operations. Only authorised employees, contractors and visitors are allowed entry to the data centres. Only authorised employees and contractors are permitted to request electronic card key access to these facilities. Data centre electronic card key access requests must be made in advance and in writing, and require the approval of authorised data centre personnel. All other entrants requiring temporary data centre access must: (i) obtain approval in advance from authorised data centre personnel for the specific data centre and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data centre access record identifying the individual as approved.

On-site Data Centre Security Devices. Google's data centres employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorised activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorised access throughout the business operations and data centres is restricted based on zones and the individual's job responsibilities. The fire doors at the data centres are alarmed. CCTV cameras are in operation both inside and outside the data centres. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data centre building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centres connect the CCTV equipment. Cameras record on-site via digital video recorders 24 hours a day,

7 days a week. The surveillance records are retained for at least 7 days based on activity. b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's administrators and users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorised persons to access data they are authorised to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralised access management system to control personnel access to production servers, and only provides access to a limited number of authorised personnel. LDAP, Kerberos and a proprietary system utilising digital certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimise the potential for unauthorised account use. The granting or modification of access rights is based on: (i) the authorised personnel's job responsibilities; (ii) job duty requirements necessary to perform authorised tasks; and (iii) a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.

3) Data

a) Data Storage, Isolation & Authentication.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centres. Google logically isolates each customer's data. A central authentication system is used across all Services to increase uniform security of data.

b) Decommissioned Disks and Disk Destruction Guidelines.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Data Destruction Guidelines") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Data Destruction Guidelines.

(a) Pseudonymous Data.

Online advertising data are commonly associated with online identifiers which on their own are considered 'pseudonymous' (i.e. they cannot be attributed to a specific individual without the use of additional information). Google has a robust set of policies and technical and organisational controls in place to ensure the separation between pseudonymous data and personally identifiable user information (i.e. information that could be used on its own to directly identify, contact, or precisely locate an individual), such as a user's Google account data. Google policies only allow for information flows between pseudonymous and personally identifiable data in strictly limited circumstances.

(b) Launch reviews.

Google conducts launch reviews for new products and features prior to launch. This includes a privacy review conducted by specially trained privacy engineers. In privacy reviews, privacy engineers ensure that all applicable Google policies and guidelines are followed, including but not limited to policies relating to pseudonymisation and data retention and deletion.

4) Personnel Security

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labour law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role. Google's personnel will not process Customer Personal Data without authorisation.

5) Subprocessor Security

Prior to onboarding further Subprocessors, Company procures that Google will (i) conduct an audit of the security and privacy practices to ensure the Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide; and (ii) enter into appropriate security, confidentiality and privacy contract terms with the Subprocessors, subject to the requirements set out in Section 10.3 (Requirements for Subprocessor Engagement).

Appendix 3: Interpretation of Customer SCCs

Customer SCC's clause reference	Interpretation
Clause 7 – Optional docking clause	Clause is not included.
Clause 9 – Use of sub-processors	OPTION 2: GENERAL WRITTEN AUTHORISATION is chosen and the time period for prior notice of Subprocessor changes will be 14 days.
Clause 11 - Redress	The optional paragraph within Clause 11 is removed.
Clause 17 – Governing law	OPTION 1 is chosen for MODULE ONE, MODULE TWO AND MODULE THREE, and the Member State where the Customer is located shall be included into Clause 17 where a Member State is required to be specified. England and Wales shall be included into Clause 17 in the event MODULE FOUR applies.

18 – Choice of forum and jurisdiction	Ireland shall be included into Clause 18 where a Member State is required to be specified for MODULE ONE, MODULE TWO AND MODULE THREE. England and Wales shall be included into Clause 18 in the event MODULE FOUR applies.
Part A, Annex I – list of Parties	For transfers from the Customer to the Company, the Customer identified as the data exporter and for transfers from the Company to the Customer, the Company identified as the data exporter; and For transfers from the Customer to the Company, the Company identified as the data importer and for transfers from the Company to the Customer, the Customer identified as the data importer.
Part B, Annex I – description of transfer	Populated with the relevant details of Section 9 (Data Transfers) and Appendix 1 (Subject Matter and Details of the Data Processing) of the Data Processing Terms.
Part C, Annex I – competent supervisory authority	'Irish DPC' shall be included where a competent supervisory authority is required to be specified.
Annex II – technical and organisational measures	As set out in Appendix 2 (Security Measures) of the Data Processing Terms.
Annex III – list of sub-processors	Populated with the list of Subprocessors set out in the Order Form and/or privacy.google.com/businesses/subprocessors.

Appendix 4: Compliance with UK GDPR

Pursuant to Section 9 of the Data Processing Terms, in connection with any Restricted European Transfers which are subject to the UK GDPR the Parties agree to be bound by the International Data Transfer Addendum ("Addendum") to the EU Commission Standard Contractual Clauses (VERSION B1.0, in force 21 March 2022) (the "Approved EU SCCs" also referred to as the "Customer SCCs" in the Data Processing Terms of the Agreement) which is, upon signature of the Order Form, incorporated into the Data Processing Terms of the Agreement together with the following information:

Table 1 is populated with the Parties to the Agreement and the contact details found in the Order Form.

Table 2 has the following option selected: 'The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information', and the details below shall read as follows:

Date: The same date as the Agreement between the Parties pursuant to which the Restricted European Transfer takes place.

Reference (if any): The Customer SCCs as incorporated into the Agreement by virtue of the Data Processing Terms, and populated by the terms set out in Appendix 3

(Interpretation of the Customer SCCs) of the Data Protection Terms of the Agreement.

Table 3 is populated with the relevant details found in the Order Form, Appendix 1 (Subject Matter and Details of the Data Processing), Appendix 2 (Security Measures) and Appendix 3 (Interpretation of the Customer SCCs) of the Data Processing terms of the Agreement.

Table 4 has the following option selected: ‘Data Exporter’.

ANNEX C, SCHEDULE 1 – PERMITTED SUPPLIER SUBPROCESSORS

Pursuant to Section 10.2 of the Data Processing Terms, the Company will engage the following Subprocessor(s) in connection with the performance of the additional Services set out above:

Name/Address (Set out here the name and registered address of the Sub-Processor)	**Services** (Set out here the Services that they will undertake in relation to Customer Personal Data)	**Location/Transfers** (Set out here the location in which the entity will process the Customer Personal Data, indicating where and from whom this has been transferred where relevant)	**Mechanism**	**Duration**
Google Analytics (360) Google LLC *1600 Amphitheatre Parkway* *Mountain View* *CA 94043* United States	Google is a full stack digital services company. The Google Analytics (360) platform is a web analytics service that reports on how users reach and interact with a website or application. If the features are activated, the platform can also be used to generate audiences for Google's advertising platforms (AdWords, DoubleClick) and website optimisation tool (Optimize). Activation of these features will also surface aggregated demographic data	Google may store and process Customer Personal Data in the United States of America and any other country in which Google or any of its Subprocessors maintains facilities. Information about the locations of Google data centres is available at *www.google.com/about/data-centers/inside/locations/index.html*.	EEA SCCs	Duration of Agreement

	gathered from Google services within Google Analytics (360). Google can also facilitate the transfer of personal data from Google Analytics (360) to its Analytics Data Warehouse (BigQuery) on the Google Cloud Platform (GCP). This processing activity is only available within the 360 version of the product. Client personal data is collected through *HTTP requests to the Google servers*. Google have summarised the types of personal data they process here: *https://privacy.google.com/businesses/adsservices/* The Client may also pass custom data into Google Analytics (360), provided it complies with the following policy which does allow for additional personal data to be sent: *https://support.google.com/analytics/answer/7686480* Personal data is also processed for the purpose of controlling access to the platform.			

Google Tag Manager (360) Google LLC *1600 Amphitheatre Parkway* *Mountain View* *CA 94043* United States	Google is a full stack digital services company. The Google Tag Manager (360) platform is a Tag Management System (TMS) that enables the Client to deploy marketing tags on a website or application from a centralised repository, based on logic-based rules. Google have summarised the types of personal data they process here: *https://privacy.google.com/businesses/adsservices/* However, the solution does not surface this data in any way to the TMS users, neither via the user interface nor the Application Programming Interface (API). TMS users may only view and edit tagging configuration data. The configuration of these tags may influence how personal data is sent to other platforms.	Google may store and process Customer Personal Data in the United States of America and any other country in which Google or any of its Subprocessors maintains facilities. Information about the locations of Google data centres is available at *www.google.com/about/data-centers/inside/locations/index.html*.	EEA SCCs	Duration of Agreement

	Personal data is also processed for the purpose of controlling access to the platform.			
Google Analytics for Firebase Google LLC 1600 Amphitheatre Parkway Mountain View CA 94043 United States	Google is a full stack digital services company. The Google Analytics for Firebase platform is a website application and mobile application analytics service that tracks and reports on how users reach and interact with an application. If the platform is integrated with advertising platforms Firebase (AdWords, DoubleClick), the platform can also be used to generate audiences for targeting. This includes Google Analytics for Firebase's app optimisation tool (Remote Config). Google Analytics for Firebase automatically collects, and surfaces aggregated demographic data gathered from Google services	Google may store and process Client Personal Data in the United States of America and any other country in which Google or any of its Subprocessors maintains facilities. Information about the locations of Google data centres is available at: www.google.com/about/datacenters/inside/locations/index.html	EEA SCCs	Duration of Agreement

	based on device identifiers if each demographic bracket aggregation is surfacing data for at least 10 users. Google Analytics for Firebase can also facilitate the transfer of personal data to its Analytics Data Warehouse (BigQuery) on the Google Cloud Platform (GCP), if linked. This processing activity is only available within the Blaze (PAYG) version of the product. Client personal data is collected using platform specific SDKs and APIs. Google have summarised the types of personal data they process here: https://privacy.google.com/businesses/adsservices/ The Client may also pass custom data into Google Analytics for Firebase to be processed, provided it complies with the following policy which does allow for additional personal data to be sent: https://support.google.com/analytics/answer/7686480			

	Personal data is also processed for the purpose of controlling access to the platform.			