Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 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	384174257894329
Call-Off Contract reference	K280022248
Call-Off Contract title	Google Analytics 360 (Premium 2024)
Call-Off Contract description	Under the current G-Cloud13 contract, DVSA currently have the provision for 300 – 400 million hits to be processed each month within the paid GA360 Account. Any hits processed in free accounts are not in scope and will not be allocated to this monthly quota. The supplier will provide DVSA with the relevant licences allowing the DVSA to access the Google Analytics 360 software for the defined DVSA accounts/properties, as per the G-Cloud13 contract.
Start date	1st January 2024
Expiry date	31st December 2024
Call-Off Contract value	£83,000.00
Charging method	BACS
Purchase order number	TBC

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	XXXXXX Redacted under FOIA section 40 XXXXXX Redacted under FOIA section 40 XXXXXX Redacted under FOIA section 40 Unity Square, Queensbridge Rd Nottingham Nottinghamshire NG2 2GD
To the Supplier	Merkle UK One Limited XXXXXX Redacted under FOIA section 40 10 Triton Street, London, NW13BF United Kingdom Company number: 04238272
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: XXXXXX Redacted under FOIA section 40
Name: XXXXXX Redacted under FOIA section 40
Email: XXXXXX Redacted under FOIA section 40
Phone: XXXXXX Redacted under

FOIA section 40

For the Supplier:

Title: XXXXXX Redacted under FOIA section 40
Name: XXXXXX Redacted under FOIA section 40
Email: XXXXXX Redacted under FOIA section 40
Phone: XXXXXX Redacted under FOIA section 40

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01/01/2024 and is valid for 12 months.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).

Extension period	There are no extension options available for this agreement.

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 2: Cloud software
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: ● 12 annual service days ● Google Analytics Support ● Google Analytics Implementation Consulting ● Google Analytics 360 Suite Product Support ● Tag Management Consulting ● Data Visualisation Assistance
Additional Services	Not applicable
Location	Not applicable
Quality Standards	Not applicable
Technical Standards:	Not applicable
Service level agreement:	As outlined in section 3 of the specification
Onboarding	Not applicable as this is a renewal of existing service

Offboarding	The offboarding plan for this Call-Off Contract will be agreed when successor arrangements have been determined
Collaboration agreement	Not applicable.
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed £500,000. The annual total liability for Buyer Data Defaults will not exceed £200,000 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 for all other Defaults will not exceed £200,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.

Insurance	The Supplier insurance(s) required will be: ● A minimum insurance period of 1 year following the expiration or Ending of this Call-Off Contract
Buyer's responsibilities	Buyer shall provide the following as outlined within the Call-Off document: • Service Level Agreements • Point of contact for day to day communication • Access to developer resource and Google Analytics, as well as necessary development environments
Buyer's equipment	The Buyer's equipment is to be used with this Call-Off Contract. The Buyer will be responsible for all equipment required to access to Google Analytics. The Buyer's equipment to be used with this Call-Off Contract includes PC's, laptops and other devices used to access Google Analytics. The Buyer's users will connect to the solution via the internet; it is assumed that all end users will already have internet access. The Suppliers does not assume any responsibility for the performance of the public internet nor any infrastructure at the Buyer's offices/locations

Supplier's information

Subcontractors or partners	None

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS Transfer
Payment profile	The payment profile for this Call-Off Contract is monthly up front.
Invoice details	The Supplier will issue electronic invoices **monthly up front**. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Invoices will be sent to SSa.invoice@sharedservicesarvato.co.uk
Invoice information required	All invoices must include: Purchase order, Project reference

Invoice frequency	Invoice will be sent to the Buyer monthly
Call-Off Contract value	The total value of this Call-Off Contract is £83,000 + Any additional overage charges
Call-Off Contract charges	£6916.66 monthly

Additional Buyer terms

Performance of the Service	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones as per the specification to the requirement and the contract.
Guarantee	N/A

Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	N/A
Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A

Personal Data and Data Subjects	As per Annex 1.and Schedule 8
Intellectual Property	N/A
Social Value	N/A

1. Formation of contract

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

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

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

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

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

Signed	Supplier	Buyer

Name	XXXXXX Redacted under FOIA section 40	XXXXXX Redacted under FOIA section 40
Title	XXXXXX Redacted under FOIA section 40	XXXXXX Redacted under FOIA section 40
Signature	XXXXXX Redacted under FOIA section 40	XXXXXX Redacted under FOIA section 40
Date	01/03/2024	01/03/2024

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

Customer Benefits

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

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

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

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

- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

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

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

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

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

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'FW2', where '2' is the Framework Agreement clause number.

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

9.8.1 premiums, which it will pay promptly
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

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

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

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

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

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

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the

Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

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

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

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

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-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:

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

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

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

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls

process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

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

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

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

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

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

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29. 2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

29.5.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7 and Schedule 8 GMP reseller terms.

Schedule 1: Services

Statement%20of%20
requirements%20Goo

Services are defined in the specification embedded above.

Schedule 2: Call-Off Contract charges

XXXXXX Redacted under FOIA section 43

Charges are outlined in the quotation embedded above.

Schedule 3: Collaboration agreement

N/A

Schedule 4: Alternative clauses

N/A.

Schedule 5: Guarantee

N/A

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR

Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.

Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium ● a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.

Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the UK GDPR.

Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	● induce that person to perform improperly a relevant function or activity
	● reward that person for improper performance of a relevant function or activity
	● commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.

Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.

Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-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.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

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

Annex 1: Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are: XXXXXX Redacted under FOIA section 40 from the Department of Transport 3rd Floor, One Priory Square, Hastings, East Sussed, TN34 1EA. Email: XXXXXX Redacted under FOIA section 40

The Representative of the DPO at DVSA is the Data Protection Manager, XXXXXX Redacted under FOIA section 40. Unity Square, Queens Bridge Road, Nottingham, NG2 1AY. Email: XXXXXX Redacted under FOIA section 40

1.2 The contact details of the Supplier's Data Protection Officer are: XXXXXX Redacted under FOIA section 40

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

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

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below *Personal data may be shared when support tickets are raised*. *The supplier will also have an understanding of our account/property numbers and how many hits are being processed against these.*

Duration of the Processing	*As required throughout the contract period. 1 year with no options to extend for an additional year.*
Nature and purposes of the Processing	*The nature of the processing is expected to include:* *Collection – as part of staff raising support tickets.*
Type of Personal Data	Names, work email addresses, job roles, phone numbers.

Categories of Data Subject	*Staff (including volunteers, agents, and temporary workers).*

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*At the end of the contract the contract owner will advise what data should be returned and what can be deleted appropriately on expiry of the contract.*

Annex 2: Joint Controller Agreement

N/A.

Schedule 8

SCHEDULE 8: GA360 TERMS

GA360 Terms set out in this Schedule are correct as of the Start Date. The parties agree and acknowledge that (i) Notwithstanding anything stated in these Terms comprising Annex A, B, C or D and Exhibit A) nothing in this Schedule 8 amends or replaces the hierarchy of interpretation set out in Clause 1.4 of the Order Form in Part A which will continue to apply in full and (ii) these Terms are based on pass-down Google terms. If Google updates the terms between Google and the Supplier, to the extent that those terms relate to the services supplied under this Call-off Contract to the Buyer, the parties shall, where consistent with the Call Off Contract (and provided there is no change to the hierarchy of interpretation set out in Clause 1.4 of the Order Form in Part A), implement such change via clause 32 (Variation) at no cost to the Buyer (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.

For the avoidance of doubt and not withstanding any definition other definition in Annex A, B, C or D or Exhibit A, the following terms in any part of this Schedule 8, shall have the following meaning
Order Form and Call Off Contract shall mean the terms set out at Part A and Part B,
“Company” shall mean the Supplier,
“Customer” shall mean the Buyer,
“Effective Date” shall mean the Start Date.

ANNEX A - GMP RESELLER TERMS

Check the GMP Reseller Terms (comprising the General Platform 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, 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) as applicable to the Services, the GMP Advertising Service Specific Terms or the GA360 Service Specific Terms, and (3) 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

DEFINTIONS & INTERPRETATION.

In the Agreement (defined below), subject to the hierarchy of interpretation set out in Clause 1.4 of the Order Form (Part A), the following terms are defined as:

“Ad(s)” means advertising content.

“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.

“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).

“Agreement” means the Order Form together with the GMP Reseller Terms and, any additional terms accepted within the user interface.

“Anti-Bribery Laws” means all applicable commercial and public anti-bribery laws, including but not limited to the UK Bribery Act 2010.

“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.

“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.
“Campaign Manager Network” means an infrastructure within the Campaign Manager Service designed to allow Customer to segment its online advertising delivery and data collections.
“Campaign Manager UI” means the Campaign Manager Service user interface.
“Company” means the ‘Company’ detailed in the Order Form.
“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.
“CPM” means cost per 1,000 impressions.
“Customer” means the ‘Customer’ detailed in the Order Form.
“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).
“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).
“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.
“Data Processing Terms” means the terms contained at the following URL: https://legal.dentsu.com/googlereseller#data-processing-terms.
“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).
“Data Provider” means a provider of Third-Party Data. , each Data Provider will retain all proprietary rights in and to its respective Third-Party Data.
“Display & Video 360 UI” means the Display & Video 360 Service user interface.
“Effective Date” has the meaning set out in the Order Form (as referred to as the Start Date in this Agreement).
“End Users” means individual human end users of a Target Property (N/A for the purpose of this Agreement).
“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.
“Exchange Spend” in N/A for the purpose of this Agreement.
“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.
“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.
“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.
“GDPR” means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

“GMP Reseller Terms” means these ‘General Platform Terms’ and the ‘GMP Advertising Service Specific Terms’ and the ‘GA360 Service Specific Terms’ (as applicable).
“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.
“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.
“Google” means Google Ireland Limited (CRN 368047) Gordon House, Barrow Street, Dublin 4, Dublin, unless otherwise notified to Customer from time to time.
“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 provided to Customer (in each case, as updated from time to time).
“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.
“Initial Term” means from the Start Date to the Expiry Date as set out in the Order Form.
“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.
“Media” means online advertising inventory made available for purchase to Customer via the Display & Video 360 Service.
“Media Provider” means an advertising exchange, network, web publisher or other provider of Media.
“Monthly Service Fees” for a Service are the Service Fees payable by Customer with respect to that Service in a certain month.
“Non-Exchange Spend” is not applicable to the Call Off Contract.
“Order Form” means the Order Form at Part A that incorporates, on the terms as set out in the Call Off Contract, these GMP Reseller Terms and sets forth pricing and other terms with respect to a particular Service.
“Personal Data” has the meaning given to it in the GDPR.
“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.
“Renewal Term” is not applicable to this Call Off Contract.
“Reseller Arrangement” means Company’s relationship with Google as described in Clause 11.10.
“Services” means the following Google Marketing Platform services: GA360 Services and/or GMP Advertising Services.
“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.
“Spend” means the sum of Customer’s Exchange Spend and Non-Exchange Spend as reported by the Display & Video 360 Service.
“Subcontractor” means a subcontractor, consultant, third-party service provider or agent engaged by the Customer in connection with its use of Services.
“Subsidiary” means any entity that is controlled by the Customer.
“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.
“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.
“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.
“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.
“Term” has the same meaning as Initial Term.
“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.
“Third Party Fees” does not apply to this Call Off Contract.
“UK GDPR” means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.
“Year” means each 12 month period commencing on the 1st June and expiring on 31st May during the Term.

THE PARTIES’ OBLIGATIONS; PROHIBITED ACTS.

Company will:
use reasonable endeavours to set up the Customer’s Services account within one month of the date of signature of the Order Form;
make available the applicable Services described in the Order Form(s) entered into by Company and Customer in accordance with these GMP Reseller Terms;
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;
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;
use current industry-standard security measures in connection with the provision of Services;
promptly notify Customer of any breach of security resulting in unauthorised third party access to the Customer Data; and
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).

Customer will:
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;
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;
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;
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;
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);
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:
discloses:

the usage of third-party technology;
the data collection and usage resulting from the Services; and
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;
includes information about End Users' options for cookie management;
complies with all applicable privacy laws, rules and regulations; and
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.

Customer:
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;
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
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.

Customer will not, and will not assist or knowingly permit any third party to:
use the Services to process Personally Identifiable Information;
pass information to Company or Google that could be used or recognised as Personally Identifiable Information;
misappropriate, misuse or abuse any part of a Service;
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);
damage or tamper with any part of a Service;
knowingly breach any Service security measure;
remove or restrict Company's access to the Google Marketing Platform during the Term; or
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.

PAYMENTS.

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.

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 this Agreement are additional to Service Fees payable under other Order Forms..

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.

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.
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).

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:

reduce Customer's access to the GMP Advertising Services to read only access; and/or
suspend each applicable Service (for which the Service Fees are overdue) after 10 days' notice to Customer; and/or
terminate the Agreement.
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.
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.

INTELLECTUAL PROPERTY.

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.

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

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.

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

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
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.

REPRESENTATIONS AND WARRANTIES.

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.

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).

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.

INDEMNIFICATION.

Customer will indemnify Company and its Affiliates against:
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;
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:
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
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");
settlement costs in relation to that Third Party Claim;
reasonable legal fees and disbursements necessarily incurred by Company or any of its Affiliates in relation to that Third Party Claim; and
reasonable costs necessarily incurred by Company or any of its Affiliates in complying with Clause 7.2.

Company will:
notify the Customer of a Third Party Claim promptly after becoming aware of it;
provide the Customer with reasonable information, assistance and cooperation in responding to and, where applicable, defending that Third Party Claim; and

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.

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.

LIMITATION OF LIABILITY.

Nothing in the Agreement will exclude or limit either Party's liability:
for death or personal injury resulting from the negligence of either Party or their servants, agents or employees;
for fraud or fraudulent misrepresentation;
for payment of sums properly due and owing to the other in the course of normal performance of the Agreement; or
for any other liability that may not otherwise lawfully be excluded or limited.

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.

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.

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:
loss of profit;
loss of anticipated savings;
loss of business opportunity;
loss of or corruption of data (except for loss or corruption of Personal Data); or
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).
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.

TERM; TERMINATION; AND SUSPENSION.

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

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):
where the breach is incapable of remedy;
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
more than twice even if the previous breaches were remedied.

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

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.

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:
suspend and/or terminate the Agreement (either in whole or in respect of those Service(s)) upon notice to Customer; or
offer the Customer any or all of the following options (in Company's sole discretion):
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
terminating the Agreement pursuant to Clause 9.5.1 and/or
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
terminating the Agreement pursuant to Clause 9.5.1 but receiving third party services similar to the relevant Services from Company.

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.

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.

EFFECT OF TERMINATION

Upon expiration or termination of the Agreement for any reason:
except as expressly stated otherwise, all rights and licences granted by each Party will cease immediately;
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
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.

In the event Clause 9.5.2 applies:
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;
Customer will continue to make payments to Company for Service Fees for the Services delivered during the Transitional Period; and

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

MISCELLANEOUS.

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.

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.

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.

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.

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.

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

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.

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).

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

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.

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.

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.

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.

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.

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

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).

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:

“Enhanced Packet” has the meaning given in Clause 1.8.

“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.

“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.

“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.

“Google Analytics” means the standard ‘Google Analytics’ product made available to customers by Google for free.

“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.

“Google Tag Manager” means the standard ‘Google Tag Manager’ product made available to customers by Google for free.

“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.

“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.

“OEP” means an “Optimize 360 Enabled Property”, which is a GA-OEP Property that is enabled for linking to Optimize 360.

“Optimize” means the standard ‘Optimize’ product made available to customers by Google for free.

“Optimize Container” means the code delivered through Optimize 360, through which Customer may serve code required to deliver modified visitor experiences.

“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.

“Platform Home” means the user interface in the Google Marketing Platform through which Customer can access certain platform-level functionality.

''Publisher'' means a third party on whose web property or content Survey Questions may be placed.

“Report” means the resulting analysis shown at www.google.com/analytics (or any other URL Company may provide from time to time).

“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.

“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.

''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.

''Sub-Property Event'' means an Event that is additionally processed by a Sub-Property and stored therein.

''Survey Questions'' means all questions submitted by Customer through Surveys 360.

"Survey Response Count" means the total number of completed surveys submitted by End Users in response to Survey Questions.
"Survey Response Data" means data submitted by End Users in response to Survey Questions.
“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.

GA360 SERVICES.

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.

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.

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.

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.

Upon termination or expiration of the Order Form (as applicable):
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
the deletion terms in the Data Processing Terms will apply to the Customer Data to the extent applicable, and Company will procure Google otherwise:
delete Customer Data if requested by Customer through the GA360 Service features made available to Customer; or
render all Customer Data externally inaccessible within a reasonable time period after receiving a written request from Customer to do so; and
Company acknowledges that continued GA360 Service use is subject to the Google Standard Product Terms; and
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.

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.

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.

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:
hereby enters into the Data Processing Terms; and
warrants that it has read and understood the Data Processing Terms and undertakes to comply with the Data Processing Terms.

CUSTOMER DATA.

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:
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;
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);
in accordance with the settings in Customer's account and the Platform Home, as applicable; and/or
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)).

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.

ANALYTICS 360.

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

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.

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").

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:
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
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.

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.

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.

OPTIMIZE 360.

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

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.

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.

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.

SURVEYS 360.

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

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").

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.

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.

TAG MANAGER 360.

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

Customer will not host the Tag Container on any domain other than the Tag Manager 360 domain or other domains which support that function without Company's prior written consent.

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.

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

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: within 4 hours of receipt at an Uptime Percentage of at least 98% for Normal GA4 Properties; within 48 hours of midnight (Pacific Time) at	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%

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/answ er/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 within 4 hours of receipt at an Uptime Percentage of at least 98% for Universal Analytics Properties that receive fewer than or equal to 2 billion Hits per calendar month and 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: 99.99% of Optimize Container requests, as most recently published by Customer; or 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 – GMP ADVERTISING SERVICE SPECIFIC TERMS
DEFINITIONS

Capitalised terms not defined in these GMP Advertising 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).

GMP ADVERTISING SERVICES.

License Grant. Upon Customer's execution of an Order Form indicating Customer's acceptance of the GMP Reseller Terms, Company grants to Customer the non-exclusive right to access and use the GMP Advertising Services subject to the terms of the Agreement.

Data Processing Terms. The Data Processing Terms will apply in respect of the Display & Video 360 Service, the Campaign Manager Service (including any add-ons to the Campaign Manager Service) and the Search Ads 360 Service.

Upon Customer's execution of an Order Form and resulting acceptance of these GMP Reseller Terms the Customer:
hereby enters into the Data Processing Terms; and
warrants that it has read and understood the Data Processing Terms and undertakes to comply with the Data Processing Terms.

With respect to each of the GMP Advertising Services:
Customer will always contact Company directly for support, and not communicate directly with Google for support;
Google may restrict, in whole or in part, the use of Tags on Customer's behalf in consent-based email publications if Google receives "spam" complaints about any of those email publications; provided that Company will ensure Customer is notified promptly following each such restriction;
Customer will not, directly or indirectly, allow any third party, other than Affiliates of Customer or Subcontractors that Customer engages to use the GMP Service(s) as contemplated hereunder, to access or have information about the user interface of any GMP Service(s); and
Customer will comply with its agreements with third parties, including Target Properties owners and advertisers, as applicable, when using the GMP Advertising Services.

CUSTOMER DATA.

As between Company and Customer, 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:
as aggregate GMP Service statistics, which will not include Personally Identifiable Information or information that identifies or would reasonably be expected to identify Customer or Target Properties;
to provide the GMP Advertising Services 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 by Google (except as otherwise expressly permitted by the Agreement) without Customer's written consent); and
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)).

The retrieval and/or provision to Customer of event-level data or archived reporting data derived from Company's use of GMP Advertising Services may result in additional fees based on storage and service costs which will be invoiced to and payable by the Customer in accordance with Clause 3 (Payments) of the General Platform Terms section of the GMP Reseller Terms.

DISPLAY & VIDEO 360 SERVICE.

With respect to the Display & Video 360 Service the terms in this Clause 4 shall apply.

Customer hereby represents and warrants that:
each of its Ad Specifications and other information entered into the Display & Video 360 Service are true and correct in all material respects;
it shall comply with the Display & Video 360 Service Policies attached hereto at Exhibit A; and
it will not, and will not assist or knowingly permit any third party to analyse, decompile, track or otherwise determine the source or location of any Third-Party Data.

Without prejudice to Customer's obligations under this Agreement, if Customer uses the Display & Video 360 Service for interest-based advertising, it must: (i) have all rights necessary to use audience data such as cookie lists; (ii) attach notices to advertisements to make clear that they are interest-based (e.g. by using an "Ad Choices" icon); (iii) disclose clearly any data collection, sharing and use on any site, app, email publication or other property that facilitates interest-based advertising; and (iv) comply with applicable advertising industry regulations, codes of practice (for example, the CAP Code in the United Kingdom) and Internet advertising industry guidelines (e.g. the Self-Regulatory Principles for Online Behavioural Advertising of the Digital Advertising Alliance, or IAB Europe's EU Framework for Online Behavioural Advertising).

Customer acknowledges that Google uses reasonable endeavours to ensure that the Display & Video 360 UI is available for Customer's use at least 99% of the time calculated on a calendar monthly basis, it being understood that Display & Video 360 UI "down" time will exclude time: (i) required for routine system maintenance (it being understood that Customer will be notified at least 2 business days' prior to any such routine maintenance); and/or (ii) resulting from technical malfunctions in the systems of Customer or of any Media Provider or Data Provider, or any other circumstances beyond Company's or Google's reasonable control (including without limitation, Internet delays, network congestion and ISP malfunctions). In the event that unscheduled down time exceeds 1% in any 3 consecutive months or in any 4 months in any 12-consecutive month period (each, a "Display & Video 360 UI Downtime Period"), Customer will have the one-time right to terminate the Order Form in respect of the Display & Video 360 Service upon 30 days' prior written notice to Company, subject to such notice being received by Company within 15 days of the end of the Display & Video 360 UI Downtime Period. The remedy set forth in this paragraph is Customer's sole remedy for any and all unavailability of the Display & Video 360 UI.

CAMPAIGN MANAGER SERVICE.

With respect to the Campaign Manager Service the terms in this Clause 5 shall apply.

Customer will remove, or cause the Target Properties to remove, all applicable Tags from the Target Properties at the completion of each Ad campaign and upon termination of Customer's access to the Campaign Manager Service the subject of an Order Form (it being understood and agreed that, notwithstanding any termination of Customer's access to the Campaign Manager Service, Customer will be liable for all use of Tags until they are removed from the Target Properties).

Use of dynamic floodlight may include without limitation the redirecting of requests from a user's browser to entities other than Google, the Customer, or the owner or operator of the Target Properties. In order for a privacy policy to comply with these GMP Reseller Terms, it must cover the collection of data through those redirects.

If Customer elects to use the proprietary request for proposal ("RFP") module (the "RFP Module"), the following terms will apply: the RFP Module is designed to facilitate media planning and buying, including without limitation selection of the Target Properties, management of the RFP process with Target Properties and generation of Insertion Orders and Media Plans. "Media Plan" means the selection of Target Properties where a campaign will be executed. "Insertion Order" means the written contract which governs the terms of placement on a Target Properties. The RFP Module is part of the Campaign Manager Service.

Customer acknowledges that Google uses reasonable endeavours to ensure that the Campaign Manager Service processes Ad requests at least 99% of the time, calculated on a calendar monthly basis as measured by Google from the data centre used by Google to serve Ads on Customer's behalf, it being understood that Ad delivery service "down" time (calculated as the difference between 100% of time in a calendar month and the actual percentage of time during that month that Ad requests are processed) will exclude time resulting from technical malfunctions in the Target Properties' systems, or
any other circumstances beyond Company or Google's reasonable control (including without limitation, Internet delays, network congestion and ISP malfunctions). Notwithstanding anything to the contrary in this Agreement, in the event that down time exceeds 1% in any month during the Campaign Manager Term, Customer will receive a reduction in fees, credited to the next month's invoice, calculated by multiplying: (i) the Average Impressions Per Hour; by (ii) the down time (rounded to the nearest hour); and by (iii) the effective CPM rate charged by Company for Ads served during that month. The "Average Impressions Per Hour" is determined by dividing the total number of Ads served in the previous month by the total number of hours in that month. The remedy set forth above in this paragraph is Customer's sole remedy for any and all unavailability of the Campaign Manager Service.
SEARCH ADS 360 SERVICE.

With respect to the Search Ads 360 Service, Customer will remove, or cause the search engine sites to remove, all applicable tracking URLs at the completion of each Ad campaign and upon the termination of Customers access to the Search Ads 360 Service (it being understood and agreed that, notwithstanding any termination of Customer's access to the Search Ads 360 Service, Customer will be liable for all use of tracking URLs until they are removed from the search engine sites).

NIELSEN DIGITAL AD RATINGS SERVICE.

If Customer opts into the Nielsen Digital Ad Ratings Service via the Display & Video 360 UI, Campaign Manager UI and/or their respective Order Form(s), the following terms will apply:
Customer hereby consents to:
Google and Nielsen Company (US), LLC and/or its Affiliates (collectively, "Nielsen") implementing Nielsen's Digital Ad Ratings product (the "DAR Product") for Customer's online advertising campaign(s) that have been enabled by Customer for measurement by the Nielsen Digital Ad Ratings Service;
Google receiving Customer's DAR Product reports ("DAR Reports") from Nielsen; and
Google using Customer's DAR Reports for purposes of: (a) improving and providing the Nielsen Digital Ad Ratings Service in connection with the GMP Advertising Services and other advertising products and services of Google and its Affiliates (collectively, "Google Group"); and (b) improving and maintaining the Google Group's inferred demographic data and demographic targeting.

Company reserves the right to limit or suspend Customer's use of the Nielsen Digital Ad Ratings Service hereunder if, as determined by Company, Customer uses the Nielsen Digital Ad Ratings Service such that a material percentage of the Nielsen Digital Ad Ratings Service Ad impressions are associated with entities outside of the country in which Customer is organised as listed in the Order Form or as otherwise agreed with Company.

Customer understands and agrees that the Nielsen Digital Ad Ratings Service may not be available for all campaigns and/or impressions.

Customer acknowledges and agrees that Nielsen owns:
all DAR Reports; and
all demographic data collected by Nielsen from Nielsen's panelists, data derived by Nielsen based on the foregoing Nielsen panelist data, demographic data licensed by Nielsen from third parties, any other data or information originating from the DAR Product, and any information that Nielsen collects to provide DAR Reports or to operate the DAR Product.

Customer may use a DAR Report solely for forecasting, Pacing (as defined below), and reporting purposes. For purposes of the Nielsen Digital Ad Ratings Service, “Pacing” means the use of information about the historic delivery of a campaign against a goal to affect the delivery of future Ad impressions for that particular campaign or other campaign(s).

Customer may share a DAR Report only with relevant third parties involved in the advertising transaction. For example, if Customer is a publisher, Customer may only disclose a DAR Report to the advertiser (or the advertiser’s agency on its behalf) that is the subject of the campaign and no other third party.

Customer will ensure that accurate dates and attribution (i.e., “Nielsen OCR” or “Nielsen DAR” or similar) are included on all permitted disclosures of the DAR Report in its entirety. External uses of a DAR Report in its entirety by Customer, such as in mass media, require Nielsen’s prior written (email sufficient) consent before disclosure.

Without limiting Customer’s obligations under the Agreement or other agreements with Company, if Customer is a publisher, Customer will ensure that the use of Tags in connection with the Nielsen Digital Ad Ratings Service is disclosed in its privacy policy or other similar user disclosure.

Customer will not combine a DAR Report and any associated DAR data with any other third party data without Nielsen’s prior written consent. For purposes of clarification, nothing herein will be interpreted to prevent Customer from internally comparing the DAR Reports to any other data set and/or sharing such comparison with Company.

Customer acknowledges and agrees that Nielsen will have the right directly to enforce the terms and conditions of Clauses 7.1.6 to 7.1.9, inclusive, of these GMP Reseller Terms governing use of the Nielsen Digital Ad Ratings Service as a third party beneficiary against Customer.

The provision of the Nielsen Digital Ad Ratings Service to Customer may be suspended at any time upon 30 days’ written notice to Customer for any reason or no reason.

Customer will indemnify Company and its Affiliates, directors, officers and employees against all liabilities, damages, losses, costs, fees (including without limitation, legal fees), and expenses relating to any allegation or legal proceeding by a third party (including without limitation, Google and Nielsen) to the extent arising from Customer’s breach of the provisions of the Nielsen Digital Ad Ratings Service.

REMARKETING SERVICE.

If Customer opts into the Remarketing Service via the Campaign Manager UI and/or the Order Form, the terms in this Clause 8 will apply.

The following capitalised terms used in this Clause 8 of these GMP Advertising Service Specific Terms have the following meanings:
“Identifiers” means collectively, identifiers (e.g., cookies, mobile advertising IDs (such as AdID or IDFA) and/or PPIDs));
“PPID” means an identifier that is unique to an End User, provided by Customer and/or a third party to Google LLC and its Affiliates as part of an Ad request;
“Remarketing Sites” means, collectively, the web sites, consent-based email publications, applications or other properties from which Compiled Lists (as defined below) will be compiled; and
“Target Sites” means, collectively, the web sites to which Customer uses the Remarketing Service to select and target Ads on the basis of the User Lists (as defined in Clause 8.6).

Customer will advise in writing each Remarketing Site and Target Site that each such site is required to contain a privacy policy that: (i) discloses (a) the usage of third-party technology; and (b) the data collection and usage resulting from the Remarketing Service; and (ii) complies with all applicable laws, rules and regulations. To the extent a Remarketing Site or Target Site may be included in an

advertising network, advertising exchange or both (as applicable), Customer will advise in writing the network owner, exchange owner or both (as applicable) rather than that Remarketing Site or Target Site.

Notwithstanding anything to the contrary in the GMP Reseller Terms, Customer will advise in writing each Remarketing Site that is a consent-based email publication that each such Remarketing Site (i.e., consent-based email publication) is required to contain a conspicuous link to a privacy policy that: (i) discloses (a) the usage of third-party technology; and (b) the data collection and usage resulting from the Remarketing Service; and (ii) complies with all applicable laws, rules and regulations.

Customer will select the Remarketing Sites on which Tags will be served under this Clause 8.

Company will procure that Google will compile, on Customer's direction and on Customer's behalf lists of Identifiers based on the various criteria Customer has selected (those lists shall be referred to as "Compiled Lists"). Customer may also provide other lists of Identifiers that were either: (i) compiled by Customer (or a third party on Customer's behalf) based on various criteria selected by Customer; or (ii) compiled by a third party and provided to Customer (provided that each of the web sites, consent-based email publications or other properties from which those Identifiers were compiled properly discloses the data collection and other uses described in this Clause 8 and complies with the privacy provisions set out in this Clause 8 and elsewhere in the GMP Reseller Terms) (these other lists shall be referred to as "Provided Lists", and together with Compiled Lists, shall be referred to as "User Lists"). A User List can consist of a combination of a Compiled List(s) (or any portion thereof) and/or a Provided List(s) (or any portion thereof).

Company may require Customer to remove or deactivate Tags that are not utilised by Customer for active Compiled Lists within 8 days following written request.

Company may suspend the Remarketing Service if Customer breaches any of the privacy policy provisions in this Clause 8.

Customer will indemnify Company, without limit, for any claim arising from a breach of this Clause 8.

Customer will not and will ensure that Subcontractor will not merge Personally Identifiable Information with information previously collected as non-Personally Identifiable Information without robust notice and prior affirmative (i.e. "opt-in") consent of the End User to such merger.

Customer may terminate any User List at any time, for any reason.

Each Party may suspend or stop using the Remarketing Service at any time upon notice to the other Party of its reasonable determination that, due to a change in law, regulation or policy, the Remarketing Service may no longer be provided to Customer or the Compiled Lists may no longer be compiled on Customer's behalf or used by Customer. Upon such suspension or notice, Customer will cease all use of Tags on, and will remove and/or cause to be removed all Tags from, each of the Remarketing Sites (it being understood and agreed that, notwithstanding the foregoing, Customer will be liable for all use of Tags until they are removed from the Remarketing Sites).

If Customer exceeds fifty million (50,000,000) Identifiers on all User Lists, Customer acknowledges and agrees that Google may reduce the size of and/or deactivate (i.e., cease the compilation of Identifiers) any one or more User Lists so that the total number of Identifiers on all User Lists is such maximum size or is less than that maximum size.

EXHIBIT A Display & Video 360 Policies
These Display & Video 360 Policies may be updated from time to time.
Creative Policies
Ads must not use the phrases "click here," "click +1" or any phrase that includes "click" as a call-to-action. This includes phrases that lead into an Ad's display URL, such as "See this site." Ads must not

contain strobing, flashing backgrounds, or otherwise distracting elements. Customer acknowledges that Google may reject or pause any Ad in its sole discretion for any or no reason, including but not limited to failure to meet exchange guidelines and Company shall not be liable for any such action taken.

Promotional Guidelines

Promotion of the following goods, services and related websites are prohibited:

escort services, prostitution, or other adult sexual services

drugs, drug paraphernalia, or aids to pass drug tests

websites that promote hacking by providing instructions or equipment to illegally access or tamper with software, servers, cell phones, or websites

tobacco or tobacco-related products (including cigarettes, cigars, tobacco pipes, rolling papers, electronic cigarettes, and e-cigarette cartridges)

gambling, sports betting, and online casino games (including gambling-related promotional products, gambling-related tutoring and educational materials, gambling related software, and gambling-related information such as tips, odds, handicapping, and sports picks)

weapons or devices designed to cause serious harm or injury, including guns, gun parts or hardware, ammunition, bombs, knives, throwing stars, and brass knuckles

websites infected with malware, or the sale of malicious software

websites that use phishing techniques (i.e. attempt to obtain users' personal information by disguising their website to look like another website)

websites that exploit online advertising systems for financial gain, distribute spam to large audiences or violate Google’s Webmaster Guidelines (available at http://www.google.com/support/webmasters/bin/answer.py?answer=35769, as modified from time to time)

III. Other Policies

Customer cannot collect site data from the Display & Video 360 Service and subsequently purchase that audience on the Display & Video 360 Service or outside of the Display & Video 360 Service. The use of deep packet inspection ("packet sniffing") in conjunction with targeting on the Display & Video 360 Service is prohibited.

ANNEX D – 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:

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;

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

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.
DURATION OF THESE DATA PROCESSING TERMS.

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.

APPLICATION OF THESE DATA PROCESSING TERMS.

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:

the processing is in the context of the activities of an establishment of Customer in the EEA or the UK; and/or
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.

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

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.

PROCESSING OF DATA.

Processor and Controller Responsibilities. The parties acknowledge and agree that:
Appendix 1 describes the subject matter and details of the processing of Customer Personal Data;
Company is a processor of Customer Personal Data under the European Data Protection Legislation;
Customer is a controller or processor, as applicable, of Customer Personal Data under the European Data Protection Legislation; and
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.

Processor Customers. If Customer is a processor:
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);
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
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).

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").

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

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.

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.

DATA DELETION.

Deletion During Term - Services With Deletion Functionality. During the Term, if:
the functionality of the Services includes the option for Customer to delete Customer Personal Data;
Customer uses the Services to delete certain Customer Personal Data; and
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.

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:
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
in respect of processing undertaken by Subprocessors, the data retention practices described at policies.google.com/technologies/ads.

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.

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.

DATA SECURITY.

Security Measures and Assistance.

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").

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

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.

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:
implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Security Measures);
complying with the terms of Section 7.2 (Data Incidents); and
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.
Customer warrants and undertakes that it is satisfied that:

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
the Company and Subprocessors have sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

Data Incidents.

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.

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.

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.

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.

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.

Customer's Security Responsibilities and Assessment.

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): Customer is responsible for its use of the Services, including:
making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data; and
securing the account authentication credentials, systems and devices Customer uses to access the Services; and
Company has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Company's and its Subprocessors' systems.

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.

Reviews and Audits of Compliance.

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.

Customer's Audit Rights.

Subject to reasonable written advance notice from the Customer the Company shall:
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: 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
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);
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
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.

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

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.

DATA SUBJECT RIGHTS.

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,
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
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.
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:
providing details of the functionality of the Services;
complying with the commitments set out in Section 8.1 (Responses to Data Subject Requests); and
if applicable to the Services, making available Data Subject Tools.

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.

DATA TRANSFERS.

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.

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:
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
if Company has not adopted an Alternative Transfer Solution for any Restricted European Transfers, then:
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,
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.

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).

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.

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

SUBPROCESSORS.

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.

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

Requirements for Subprocessor Engagement. When engaging any Subprocessor, Company will ensure via a written contract that:
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);
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
remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

OPPORTUNITY TO OBJECT TO SUBPROCESSOR CHANGES.

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.

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.

CONTACTING COMPANY; PROCESSING RECORDS.

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.

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.

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.

LIABILITY.

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.

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).

EFFECT OF THESE DATA PROCESSING TERMS.

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:
the Customer SCCs (if applicable);
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.

Subject to the amendments in these Data Processing Terms, the Agreement remains in full force and effect.
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.
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.
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.

CHANGES TO THESE DATA PROCESSING TERMS.

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.

Changes to Data Processing Terms. Company may change these Data Processing Terms if the change:
is expressly permitted by these Data Processing Terms, including as described in Section 15.1 (Changes to URLs);
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;
reflects a change in the name or form of a legal entity;
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
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.

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:

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

if Google has not adopted or has informed Company that Google is no longer adopting an Alternative Transfer Solution for any Restricted Transfers, then:

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

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:
Tightly controlling the size and make-up of Google's attack surface through preventative measures;
Employing intelligent detection controls at data entry points; and
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.
Data

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.
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.

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.

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.

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.

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 D, 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 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:	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/datacenters/inside/locations/index.html.	EEA SCCs	Duration of Agreement

	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. Personal data is also processed for the purpose of controlling access to the platform.	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/datacenters/inside/locations/index.html.	EEA SCCs	Duration of Agreement

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 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	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

	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.			