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 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. **"Customer Personal Data"** means personal data that is processed by Company on behalf of Customer in the provision of the Services.

2.4. **"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 log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

2.5. **"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).

2.6. **"EEA"** means the European Economic Area.

2.7. **"European Data Protection Legislation"** means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

2.8. **"European or National Laws"** means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and/or (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).

2.9. **"Google Security Measures"** has the meaning given in Section 7.1.2 (Google Security Measures).

2.10. **"Google Subprocessors"** has the meaning given in Section 10.1 (Consent to Subprocessor Engagement).

2.11. **"Google Entity"** means Google LLC (formerly known as Google Inc.), Google or any other Affiliate of Google LLC.

2.12. **"Model Contract Clauses"** means the terms at https://privacy.google.com/businesses/processorterms/mccs, which are standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the EU GDPR.

2.13. **"Non-European Data Protection Legislation"** means data protection or privacy laws in force outside the EEA, Switzerland and the UK.

2.14. **"Notification Email Address"** means the email address (if any) 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.

2.15. **"Security Documentation"** means any security certifications or documentation that Company may make available in respect of the Services.

2.16. **"Security Measures"** has the meaning given in Section 7.1.1 (Security Measures).
2.17. **"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.
2.18. **"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.
2.19. **"Term"** means the period from the Effective Date until the end of Company's provision of the Services under the Agreement.
2.20. **"Third Party Subprocessors"** has the meaning given in Section 10.1 (Consent to Subprocessor Engagement).
2.21. 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 Model Contract Clauses.
2.22. 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.
2.23. Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3. DURATION OF THESE DATA PROCESSING TERMS.

3.1. These Data Processing Terms will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon deletion of all Customer Personal Data by Company and its Subprocessors as described in these Data Processing Terms.

4. APPLICATION OF THESE DATA PROCESSING TERMS.

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

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

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

5. PROCESSING OF DATA

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

5.2. Authorisation by Third Party Controller. If Customer is a processor, Customer warrants to Company that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of Company (and in turn Subprocessors) as another processor, have been authorised by the relevant controller.

5.3. Customer's Instructions. By entering into these Data Processing Terms, Customer instructs Company to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and any related technical and/or support services; (b) as further specified via Customer's use of the Services

(including in the settings and other functionality of the Services) and any related technical and/or support services; (c) as documented in the form of the Agreement, including these Data Processing Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Company as constituting instructions for purposes of these Data Processing Terms.

5.4. Compliance with Instructions. Company will comply with the instructions described in Section 5.3 (Customer's Instructions) (including with regard to data transfers) unless European or National Laws to which Company is subject require other processing of Customer Personal Data by Company, in which case Company will inform Customer (unless any such law prohibits Company from doing so on important grounds of public interest).

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

6. DATA DELETION.

6.1. Deletion During Term - Services With Deletion Functionality. During the Term, if:
6.1.1. the functionality of the Services includes the option for Customer to delete Customer Personal Data;
6.1.2. Customer uses the Services to delete certain Customer Personal Data; and
6.1.3. the deleted Customer Personal Data cannot be recovered by Customer (for example, from the "trash"),

then Company will delete such Customer Personal Data from its systems as soon as reasonably practicable and within a maximum period of 180 days, unless European or National Laws require storage.

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

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

6.4. Deletion on Term Expiry. On expiry of the Term, Customer instructs Company to delete all Customer Personal Data (including existing copies) from its systems 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 or National Laws require storage.

7. DATA SECURITY

7.1. Security Measures and Assistance.

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

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

7.1.3. Security Compliance by Company personnel. Company will 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, including ensuring that all persons authorised to

process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.4. Security Assistance. Customer agrees that 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 any obligations of Customer in respect of security of personal data and personal data breaches, including (if applicable) Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

7.1.4.1. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Security Measures);

7.1.4.2. complying with the terms of Section 7.2 (Data Incidents); and

7.1.4.3. providing Customer with the Security Documentation in accordance with Section 7.4.1 (Reviews of Security Documentation) and the information contained in these Data Processing Terms.

7.1.5. Customer warrants and undertakes that it is satisfied that:

7.1.5.1. the Company and Subprocessors processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Company to process Customer Personal Data; and

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

7.2. Data Incidents.

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

7.2.2. Details of Data Incident. Notifications made under Section 7.2.1 (Incident Notification) will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and may include recommended steps for Customer to take to address the Data Incident.

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

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

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

7.3. Customer's Security Responsibilities and Assessment.

7.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Company's obligations under Sections 7.1 (Security Measures and Assistance) and 7.2 (Data Incidents):

7.3.1.1. Customer is responsible for its use of the Services, including:

7.3.1.1.1. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data; and

7.3.1.1.2. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

7.3.1.2. Company has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Company's and its Subprocessors' systems.

7.3.2. Customer's Security Assessment. Customer acknowledges and agrees that (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) 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.

7.4. Reviews and Audits of Compliance.

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

7.4.2. Customer's Audit Rights.

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

7.4.2.1.1. permit the Customer to conduct (and shall contribute to) audits and inspections of its systems and processes in relation to the processing of Customer Personal Data subject to the Customer ensuring:

7.4.2.1.1.1. that such audit or inspection is undertaken during normal business hours and with minimal disruption to the Company's business and the business of other clients of the Company; and

7.4.2.1.1.2. that all information obtained or generated by the Customer or its auditor(s) in connection with such audits and inspections is kept strictly confidential (save for disclosure to a regulatory authority or as otherwise required by Data Protection Laws);

7.4.2.1.2. give the Customer such information as is reasonably necessary to verify that the Company is in compliance with its obligations under Data Protection Laws; and

7.4.2.1.3. co-operate and assist the Customer with any data protection impact assessments and consultations with any regulatory authority that the Customer reasonably considers are relevant pursuant to Data Protection Laws in relation to the Customer Personal Data.

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

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

7.5. No Modification of Model Contract Clauses. If the Model Contract Clauses apply under Section 9.2 (Transfers of Data), nothing in this Section 7.4 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Google LLC under the Model Contract Clauses.

8. DATA SUBJECT RIGHTS.

8.1. Responses to Data Subject Requests. Company will notify Customer if it receives a request from or on behalf of a data subject of Customer Personal Data to exercise any of the rights given to data subjects by Data Protection Laws. Notwithstanding the aforementioned,

8.1.1. if the request is made via a Data Subject Tool, Google Subprocessors will respond directly to the data subject's request in accordance with the standard functionality of that Data Subject Tool; or

8.1.2. if the request is not made via a Data Subject Tool, Customer or the Subprocessors will advise the data subject to submit his/her request to Customer,

and Customer will be responsible for responding to such request.

8.2. Data Subject Request Assistance. Customer agrees that Company will (taking into account the nature of the processing of Customer Personal Data and, if applicable, Article 11 of the GDPR) provide reasonable assistance to Customer in fulfilling any obligation of Customer to respond to requests by data subjects, including (if applicable) Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

8.2.1. providing details of the functionality of the Services;

8.2.2. complying with the commitments set out in Section 8.1 (Responses to Data Subject Requests); and

8.2.3. if applicable to the Services, making available Data Subject Tools.

9. DATA TRANSFERS.

9.1. Data Storage and Processing Facilities. Customer agrees that Company or its Subprocessors may, subject to Section 9.2 (Transfers of Data), store and process Customer Personal Data in any country in which Company or any of its Subprocessors maintains facilities.

9.2. Transfers of Data. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data from the EEA, Switzerland or the UK to any third country that is not subject to an adequacy decision under the European Data Protection Legislation:

9.2.1. Customer (as data exporter) will be deemed to have entered into the Model Contract Clauses with Google LLC (as data importer);

9.2.2. the transfers will be subject to the Model Contract Clauses; and

9.2.3. Company will ensure that Google LLC complies with its obligations under such Model Contract Clauses in respect of such transfers.

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

10. SUBPROCESSORS.

10.1. Consent to Subprocessor Engagement. Customer specifically authorises the engagement of Google and its Affiliates as Subprocessors and further Subprocessors (together the "**Google Subprocessors**"). In addition, Customer generally authorises the engagement of any other third parties as Subprocessors and further Subprocessors (together the "**Third Party Subprocessors**"). If the Model Contract Clauses apply under Section 9.2 (Transfers of Data), the above authorisations constitute Customer's prior written consent to the subcontracting by Company of the processing of Customer Personal Data.

10.2. Information about Subprocessors. Information about Subprocessors may be set out in the Order Form and can otherwise be found at privacy.google.com/businesses/subprocessors.

10.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Company will ensure via a written contract that:

10.3.1. the Subprocessor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Data Processing Terms) and, if applicable under Section 9.2 (Transfers of Data), the Model Contract Clauses;

10.3.2. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Subprocessor; and

10.3.3. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11. OPPORTUNITY TO OBJECT TO SUBPROCESSOR CHANGES.

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

11.2. Customer may object to any new Third Party Subprocessor by terminating the Agreement 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 Third Party Subprocessor as described in Section 11.1. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. CONTACTING COMPANY; PROCESSING RECORDS.

12.1. Contacting Company. Customer may contact Company in relation to the exercise of its rights under these Data Processing Terms via email to dpo@dentsu.com or via such other means as may be provided by Company from time to time.

12.2. Processing Records. Customer acknowledges that Company is required under the GDPR to: (a) collect and maintain records of certain information, including 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 (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.

13. LIABILITY.

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

13.2. Liability if the Model Contract Clauses Apply. If the Model Contract Clauses apply under Section 9.2 (Transfers of Data), the total combined liability of Company and Google Subprocessors towards Customer under or in connection with the Agreement and the Model Contract Clauses combined will be subject to Section 13.1 (Liability Cap).

14. THIRD-PARTY BENEFICIARY.

14.1. Google Subprocessors, including Google LLC where the Model Contract Clauses apply under Section 9.2 (Transfers of Data) will be a third-party beneficiary of Sections 6.4 (Deletion on Term Expiry), 8.1 (Responses to Data Subject Requests), 9.2 (Transfers of Data), 10.1 (Consent to Subprocessor Engagement), and 13.2 (Liability if the Model Contract Clauses Apply). To the extent this Section 14 (Third-Party Beneficiary) conflicts or is inconsistent with any other clause in the Agreement, this Section 14 (Third-Party Beneficiary) will apply.

15. EFFECT OF THESE DATA PROCESSING TERMS.

15.1. If there is any conflict or inconsistency between the Model Contract Clauses, the Additional Terms for Non-European Data Protection Legislation, and the remainder of these Data Processing Terms and/or the remainder of the Agreement, then the following order of precedence will apply:
- 15.1.1. the Model Contract Clauses;
- 15.1.2. the Additional Terms for Non-European Data Protection Legislation;
- 15.1.3. the remainder of these Data Processing Terms; and
- 15.1.4. the remainder of the Agreement.

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

16. CHANGES TO THESE DATA PROCESSING TERMS.

16.1. Changes to URLs. From time to time, Company may change any URL referenced in these Data Processing Terms and the content at any such URL, except that Company may only change the Model Contract Clauses in accordance with Sections 16.2.2 - 16.2.4 (Changes to Data Processing Terms) or to incorporate any new version of the Model Contract Clauses that may be adopted under the European Data Protection Legislation, in each case in a manner that does not affect the validity of the Model Contract Clauses under the European Data Protection Legislation.

16.2. Changes to Data Processing Terms. Company may change these Data Processing Terms if the change:
- 16.2.1. is expressly permitted by these Data Processing Terms, including as described in Section 16.1 (Changes to URLs);
- 16.2.2. reflects a change in the name or form of a legal entity;
- 16.2.3. is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or
- 16.2.4. 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.

16.3. Notification of Changes. If Company intends to change these Data Processing Terms under Section 16.2.3 or 16.2.4, 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 terminate the Agreement 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 16.2.3 or 16.2.4.

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 expiry 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 described in Section 5.3 (Customer's 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.

Appendix 2: Security Measures

This Appendix 2 sets out the Google Security Measures as at the Effective Date. These Google Security Measures may update 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-of-tolerance 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 diesel generator systems take over. The diesel 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.

Businesses 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.

b) Networks & Transmission.

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

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

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

i) Tightly controlling the size and make-up of Google's attack surface through preventative measures;
ii) Employing intelligent detection controls at data entry points; and
iii) Employing technologies that automatically remedy certain dangerous situations.

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

Encryption Technologies. Google makes HTTPS encryption (also referred to as TLS connection) available. Google servers support ephemeral elliptic curve Diffie Hellman cryptographic key exchange signed with RSA and ECDSA.

These perfect forward secrecy (PFS) methods help protect traffic and minimise the impact of a compromised key, or a cryptographic breakthrough.

2) Access and Site Controls

a) Site Controls.

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

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

On-site Data Centre Security Devices. Google's data centres employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorised activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorised access throughout the business operations and data centres is restricted based on zones and the individual's job responsibilities. The fire doors at the data centres are alarmed. CCTV cameras are in operation both inside and outside the data centres. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data centre building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centres connect the CCTV equipment. Cameras record on-site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for at least 7 days based on activity.

b) Access Control.

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

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

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

3) Data

a) Data Storage, Isolation & Authentication.

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

b) Decommissioned Disks and Disk Destruction Guidelines.

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

4) Personnel Security

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

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

5) Subprocessor Security

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