Google Ads Data Processing Terms

Google and the counterparty agreeing to these terms ("**Customer**") have entered into an agreement for the provision of the Processor Services (as amended from time to time, the "**Agreement**").

These Google Ads Data Processing Terms (including the appendices, "**Data Processing Terms**") are entered into by Google 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 Processor Services), from the Terms Effective Date.

If you are accepting these Data Processing Terms on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to these Data Processing Terms; (b) you have read and understand these Data Processing Terms; and (c) you agree, on behalf of Customer, to these Data Processing Terms. If you do not have the legal authority to bind Customer, please do not accept these Data Processing Terms.

1. Introduction

These Data Processing Terms reflect the parties' agreement on the terms governing the processing and security of Customer Personal Data in connection with the Data Protection Legislation.

2. Definitions and Interpretation

2.1 In these Data Processing Terms:

"**Additional Product**" means a product, service or application provided by Google or a third party that: (a) is not part of the Processor Services; and (b) is accessible for use within the user interface of the Processor Services or is otherwise integrated with the Processor Services.

"**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with, a party.

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

"**Data Incident**" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data on systems managed by or otherwise controlled by Google. "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.

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

"**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).

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

"**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.

"**Google**" means the Google Entity that is party to the Agreement.

"**Google Affiliate Subprocessors**" has the meaning given in Section 11.1 (Consent to Subprocessor Engagement).

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

"**ISO 27001 Certification**" means ISO/IEC 27001:2013 certification or a comparable certification for the Processor Services.

"**Notification Email Address**" means the email address (if any) designated by Customer, via the user interface of the Processor Services or such other means provided by Google, to receive certain notifications from Google relating to these Data Processing Terms.

"**Privacy Shield**" means the EU-U.S. Privacy Shield legal framework and the Swiss-U.S. Privacy Shield legal framework.

"**Processor Services**" means the applicable services listed at privacy.google.com/businesses/adsservices .

"**Security Documentation**" means the certificate issued for the ISO 27001 Certification and any other security certifications or documentation that Google may make available in respect of the Processor Services.

"**Security Measures**" has the meaning given in Section 7.1.1 (Google's Security Measures).

"**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 Processor Services and any related technical support.

"**Term**" means the period from the Terms Effective Date until the end of Google's provision of the Processor Services under the Agreement.

"**Terms Effective Date**" means, as applicable:

(a) 25 May 2018, if Customer clicked to accept or the parties otherwise agreed to these Data Processing Terms before or on such date; or

(b) the date on which Customer clicked to accept or the parties otherwise agreed to these Data Processing Terms, if such date is after 25 May 2018.

"**Third Party Subprocessors**" has the meaning given in Section 11.1 (Consent to Subprocessor Engagement).

2.2 The terms "**controller**", "**data subject**", "**personal data**", "**processing**", "**processor**" and "**supervisory authority**" as used in these Data Processing Terms have the meanings given in the GDPR.

2.3 Any phrase introduced by the terms "**including**", "**include**" or any similar expression will be construed as illustrative and will not limit the sense of the words preceding those terms. Any examples in these Data Processing Terms are illustrative and not the sole examples of a particular concept.

2.4 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

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

4. Application of these Data Processing Terms

4.1 **Application of Data Protection Legislation**. These Data Processing Terms will only apply to the extent that the Data Protection Legislation applies to the processing of Customer Personal Data, including if:

(a) the processing is in the context of the activities of an establishment of Customer in the EEA; and/or

(b) Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services or the monitoring of their behaviour in the EEA.

4.2 **Application to Processor Services**. These Data Processing Terms will only apply to the Processor Services for which the parties agreed to these Data Processing Terms (for example: (a) the Processor Services for which Customer clicked to accept these Data Processing Terms; or (b) if the Agreement incorporates these Data Processing Terms by reference, the Processor Services that are the subject of the Agreement).

5. Processing of Data

5.1 **Roles and Regulatory Compliance; Authorisation**.

5.1.1 **Processor and Controller Responsibilities**. The parties acknowledge and agree that:

(a) Appendix 1 describes the subject matter and details of the processing of Customer Personal Data;

(b) Google is a processor of Customer Personal Data under the Data Protection Legislation;

(c) Customer is a controller or processor, as applicable, of Customer Personal Data under the Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Customer Personal Data.

5.1.2 **Authorisation by Third Party Controller**. If Customer is a processor, Customer warrants to Google that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of Google as another processor, have been authorised by the relevant controller.

5.2 **Customer's Instructions**. By entering into these Data Processing Terms, Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Processor Services and any related technical support; (b) as further specified via Customer's use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support; (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 Google as constituting instructions for purposes of these Data Processing Terms.

5.3 **Google's Compliance with Instructions**. Google will comply with the instructions described in Section 5.2 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Google is subject requires other processing of Customer Personal Data by Google, in which case Google will inform Customer (unless that law prohibits Google from doing so on important grounds of public interest).

5.4 **Additional Products**. If Customer uses any Additional Product, the Processor Services may allow that Additional Product to access Customer Personal Data as required for the interoperation of the Additional Product with the Processor 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**.

6.1.1 **Processor Services With Deletion Functionality**. During the Term, if:

(a) the functionality of the Processor Services includes the option for Customer to delete Customer Personal Data;

(b) Customer uses the Processor Services to delete certain Customer Personal Data; and

(c) the deleted Customer Personal Data cannot be recovered by Customer (for example, from the "trash"),

then Google will delete such Customer Personal Data from its systems as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

6.1.2 **Processor Services Without Deletion Functionality**. During the Term, if the functionality of the Processor Services does not include the option for Customer to delete Customer Personal Data, then Google will comply with:

(a) any reasonable request from Customer to facilitate such deletion, insofar as this is possible taking into account the nature and functionality of the Processor Services and unless EU or EU Member State law requires storage; and

(b) the data retention practices described at www.google.com/policies/technologies/ads.

Google may charge a fee (based on Google's reasonable costs) for any data deletion under Section 6.1.2(a). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such data deletion.

6.2 **Deletion on Term Expiry**. On expiry of the Term, Customer instructs Google to delete all Customer Personal Data (including existing copies) from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

7. Data Security

7.1 **Google's Security Measures and Assistance**.

7.1.1 **Google's Security Measures**. Google will implement and maintain technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Appendix 2 (the "**Security Measures**"). As described in Appendix 2, the Security Measures include measures: (a) to encrypt personal data; (b) to help ensure the ongoing confidentiality, integrity, availability and resilience of Google's systems and services; (c) to help restore timely access to personal data following an incident; and (d) for regular testing of effectiveness. Google may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

7.1.2 **Security Compliance by Google Staff**. Google will take appropriate 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.

7.1.3 **Google's Security Assistance**. Customer agrees that Google will (taking into account the nature of the processing of Customer Personal Data and the information available to

Google) 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:

(a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

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

(c) providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in these Data Processing Terms.

7.2 **Data Incidents**.

7.2.1 **Incident Notification**. If Google becomes aware of a Data Incident, Google 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 steps Google recommends Customer take to address the Data Incident.

7.2.3 **Delivery of Notification**. Google will deliver its notification of any Data Incident to the Notification Email Address or, at Google'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 Google**. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google 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 Google's obligations under Sections 7.1 (Google's Security Measures and Assistance) and 7.2 (Data Incidents):

(a) Customer is solely responsible for its use of the Processor Services, including:

(i) making appropriate use of the Processor Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data; and

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Processor Services; and

(b) Google has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Google'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 Google as set out in Section 7.1.1 (Google's Security Measures) provide a level of security appropriate to the risk in respect of Customer Personal Data.

7.4 **Security Certification**. To evaluate and help ensure the continued effectiveness of the Security Measures, Google will maintain the ISO 27001 Certification.

7.5 **Reviews and Audits of Compliance**.

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

7.5.2 **Customer's Audit Rights**.

(a) Google will allow Customer or a third party auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under these Data Processing Terms in accordance with Section 7.5.3 (Additional Business Terms for Audits). Google will contribute to such audits as described in Section 7.4 (Security Certification) and this Section 7.5 (Reviews and Audits of Compliance).

(b) Customer may also conduct an audit to verify Google's compliance with its obligations under these Data Processing Terms by reviewing the certificate issued for the ISO 27001 Certification (which reflects the outcome of an audit conducted by a third party auditor).

7.5.3 **Additional Business Terms for Audits**.

(a) Customer will send any request for an audit under Section 7.5.2(a) to Google as described in Section 12.1 (Contacting Google).

(b) Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any audit under Section 7.5.2(a).

(c) Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any third party auditor appointed by Customer to execute any such audit.

(d) Google may object to any third party auditor appointed by Customer to conduct any audit under Section 7.5.2(a) if the auditor is, in Google's reasonable opinion, not suitably qualified

or independent, a competitor of Google or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.

(e) Nothing in these Data Processing Terms will require Google either to disclose to Customer or its third party auditor, or to allow Customer or its third party auditor to access:

(i) any data of any other customer of a Google Entity;

(ii) any Google Entity's internal accounting or financial information;

(iii) any trade secret of a Google Entity;

(iv) any information that, in Google's reasonable opinion, could: (A) compromise the security of any Google Entity's systems or premises; or (B) cause any Google Entity to breach its obligations under the Data Protection Legislation or its security and/or privacy obligations to Customer or any third party; or

(v) any information that Customer or its third party auditor seeks to access for any reason other than the good faith fulfilment of Customer's obligations under the Data Protection Legislation.

8. Impact Assessments and Consultations

Customer agrees that Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including (if applicable) Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

(a) providing the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation);

(b) providing the information contained in these Data Processing Terms; and

(c) providing or otherwise making available, in accordance with Google's standard practices, other materials concerning the nature of the Processor Services and the processing of Customer Personal Data (for example, help centre materials).

9. Data Subject Rights

9.1 **Responses to Data Subject Requests**. If Google receives a request from a data subject in relation to Customer Personal Data, Google will:

(a) if the request is made via a Data Subject Tool, respond directly to the data subject's request in accordance with the standard functionality of that Data Subject Tool; or

(b) if the request is not made via a Data Subject Tool, advise the data subject to submit his/her request to Customer, and Customer will be responsible for responding to such request.

9.2 **Google's Data Subject Request Assistance**. Customer agrees that Google will (taking into account the nature of the processing of Customer Personal Data and, if applicable, Article 11 of the GDPR) assist 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:

(a) providing the functionality of the Processor Services;

(b) complying with the commitments set out in Section 9.1 (Responses to Data Subject Requests); and

(c) if applicable to the Processor Services, making available Data Subject Tools.

10. Data Transfers

10.1 **Data Storage and Processing Facilities**. Customer agrees that Google may, subject to Section 10.2 (Transfers of Data Out of the EEA and Switzerland), 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.

10.2 **Transfers of Data Out of the EEA and Switzerland**. Google will ensure that:

(a) the parent company of the Google group, Google LLC, remains self-certified under Privacy Shield on behalf of itself and its wholly-owned U.S. subsidiaries; and

(b) the scope of Google LLC's Privacy Shield certification includes Customer Personal Data.

10.3 **Data Centre Information**. Information about the locations of Google data centres is available at www.google.com/about/datacenters/inside/locations/index.html .

11. Subprocessors

11.1 **Consent to Subprocessor Engagement**. Customer specifically authorises the engagement of Google's Affiliates as Subprocessors ("**Google Affiliate Subprocessors**"). In addition, Customer generally authorises the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**").

11.2 **Information about Subprocessors**. Information about Subprocessors is available at privacy.google.com/businesses/subprocessors .

11.3 **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Google will:

(a) ensure via a written contract that:

(i) 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 Privacy Shield; and

(ii) 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

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

11.4 **Opportunity to Object to Subprocessor Changes**.

(a) When any new Third Party Subprocessor is engaged during the Term, Google will, at least 30 days before the new Third Party Subprocessor processes any Customer Personal Data, inform 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.

(b) Customer may object to any new Third Party Subprocessor by terminating the Agreement immediately upon written notice to Google, on 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 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. Contacting Google; Processing Records

12.1 **Contacting Google**. Customer may contact Google in relation to the exercise of its rights under these Data Processing Terms via the methods described at privacy.google.com/businesses/processorsupport or via such other means as may be provided by Google from time to time.

12.2 **Google's Processing Records**. Customer acknowledges that Google 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 Google 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 the supervisory authorities. Accordingly, Customer will, where requested and as applicable to Customer, provide such information to Google via the user interface of the Processor Services or via such other means as may be provided by Google, and will use such user interface or other means to ensure that all information provided is kept accurate and up-to-date.

13. Liability

If the Agreement is governed by the laws of:

(a) a state of the United States of America, then, notwithstanding anything else in the Agreement, the total liability of either party towards the other party under or in connection with these Data Processing Terms will be limited to the maximum monetary or payment-based amount at which that party's liability is capped under the Agreement (for clarity, any exclusion of indemnification claims from the Agreement's limitation of liability will not apply to indemnification claims under the Agreement relating to the Data Protection Legislation); or

(b) a jurisdiction that is not a state of the United States of America, then 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.

14. Effect of these Data Processing Terms

If there is any conflict or inconsistency between the terms of these Data Processing Terms and the remainder of the Agreement, the terms of these Data Processing Terms will govern. Subject to the amendments in these Data Processing Terms, the Agreement remains in full force and effect.

15. Changes to these Data Processing Terms

15.1 **Changes to URLs**. From time to time, Google may change any URL referenced in these Data Processing Terms and the content at any such URL. Google may only change the list of potential Processor Services at privacy.google.com/businesses/adsservices :

(a) to reflect a change to the name of a service;

(b) to add a new service; or

(c) to remove a service where either: (i) all contracts for the provision of that service are terminated; or (ii) Google has Customer's consent.

15.2 **Changes to Data Processing Terms**. Google may change these Data Processing Terms if the change:

(a) is expressly permitted by these Data Processing Terms, including as described in Section 15.1 (Changes to URLs);

(b) reflects a change in the name or form of a legal entity;

(c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or

(d) does not: (i) result in a degradation of the overall security of the Processor Services; (ii) expand the scope of, or remove any restrictions on, Google's processing of Customer Personal Data, as described in Section 5.3 (Google's Compliance with Instructions); and (iii) otherwise have a material adverse impact on Customer's rights under these Data Processing Terms, as reasonably determined by Google.

15.3**Notification of Changes**. If Google intends to change these Data Processing Terms under Section 15.2(c) or (d), Google will inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) 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 Processor Services. If Customer objects to any such change, Customer may terminate the Agreement by giving written notice to Google within 90 days of being informed by Google of the change.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Processor 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 Google in accordance with these Data Processing Terms.

Nature and Purpose of the Processing

Google will process (including, as applicable to the Processor Services and the instructions described in Section 5.2 (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 Processor 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 collects personal data in its provision of the Processor Services; and/or
- data subjects about whom personal data is transferred to Google in connection with the Processor Services by, at the direction of, or on behalf of Customer.

Depending on the nature of the Processor 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 Google provides the Processor Services; and/or (c) who are customers or users of Customer's products or services.

Appendix 2: Security Measures

As from the Terms Effective Date, Google will implement and maintain the Security Measures set out in this Appendix 2. Google may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor 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 Processor 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 Processor 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. This is designed to prevent data from being read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media. 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:

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

2. Employing intelligent detection controls at data entry points; and

3. 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 SSL or 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 operation 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 the requestor's manager and the data centre director. All other entrants requiring temporary data centre access must: (i) obtain approval in advance from the data centre managers 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 Processor 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 Processor 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 SSH 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: the authorised personnel's job responsibilities; job duty requirements necessary to perform authorised tasks; and 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 Processor 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 Processor 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 backgrounds checks to the extent legally permissible and in accordance with applicable local labor 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

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure 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. Once Google has assessed the risks presented by the Subprocessor then, subject always to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Google Ads Data Processing Terms, Version 1.2

12 October 2017