By proceeding, you confirm that you have a business established in the territory of a member state of the European Economic Area or Switzerland, or that, for other reasons, you are subject to the territorial scope of the national implementations of Directive 95/46/EC. You further agree that if the aforementioned is not the case, this Data Processing Amendment between you and Google shall be void.

Data Processing Amendment to the Google Analytics Agreement

You agreeing to these terms ("**Customer**") and Google Inc. or Google Ireland Limited (as applicable) have entered into Google Analytics Terms of Service or an Analytics 360 Agreement, as applicable (as amended to date) (the "**Google Analytics Agreement**"). This amendment (the "**Data Processing Amendment**") is entered into by and between Customer and Google Inc. ("**Google**"), 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA as of the Effective Date and amends the Google Analytics Agreement. The "Effective Date" is the date Customer accepts this Data Processing Amendment by clicking to accept these terms.

If you are accepting on behalf of Customer, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand this Data Processing Amendment; and (iii) you agree, on behalf of the party that you represent, to this Data Processing Amendment. If you do not have the legal authority to bind Customer, please do not click the "Accept" button below.

1. Introduction

1.1 Subject to Section 1.2 below, Customer may use the Services to process Customer Personal Data in accordance with this Data Processing Amendment.

1.2 Customer may not use the Services to process Customer Personal Data which in itself personally identifies an individual (such as a name, email address or billing information), or other data which can be reasonably linked to such information by Google.

1.3 This Data Processing Amendment only applies if and to the extent that the parties process Customer Personal Data under the Google Analytics Agreement, including with respect to personal data in accordance with the Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and the member countries' national implementation.

2. Definitions

2.1 Capitalized terms used but not defined in this Data Processing Amendment will have the meaning provided in the Agreement. In this Data Processing Amendment, unless expressly stated otherwise:

"**Additional Products**" means products, services and applications (whether made available by Google or a third party) that are not part of the Services.

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

"**Agreement**" means the Google Analytics Agreement and this Data Processing Amendment.

"**Analytics 360 Agreement**" means an agreement for the provision of Analytics 360 (formerly known as Google Analytics Premium) services, comprising: (i) a DoubleClick Advertising Platform Agreement or DoubleClick Advertising and Google Analytics 360 Suite Platform Agreement; and (ii) Google Analytics Premium or Analytics 360 Order Form (as applicable).

"**Customer Personal Data**" means any Personal Data collected, transmitted, analysed or otherwise processed through the Services which concerns the characteristics and activities of users visiting web pages, apps or other properties or services linked to your Google Analytics account(s).

"**Data Protection Legislation**" means the national provisions adopted pursuant to the Directive, in the country in which the Customer is established.

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"**Google Group**" means those Google Affiliates that may be used to provide the Services to Customer.

"**Instructions**" means the written instructions of the Customer specified in the Agreement (as amended or replaced) and any subsequent instructions from the Customer to Google and acknowledged by Google.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Security Incident**" means accidental or unlawful distribution or accidental loss, alteration, or unauthorised disclosure or access to Customer Personal Data by Google or its Subprocessors.

"**Security Measures**" has the meaning given in Section 6.1 of this Data Processing Amendment.

"**Subprocessors**" means the Google Group and Third Party Suppliers.

"**Services**" means, for purposes of this Data Processing Amendment, those services defined as the "Google Analytics", "Google Analytics Premium Service" or "Analytics 360 Service" (as applicable) under the Agreement.

"**Third Party Suppliers**" means the third party suppliers engaged by the Google Group for the purposes of processing Customer Personal Data in the context of the provision of the Services. Additional information about Third Party Suppliers is available at the following URL: http://www.google.com/analytics/terms/subprocessors.html, as such URL may be updated from time to time by Google.

2.2. The terms "personal data", "processing", "controller" and "processor" shall have the meanings ascribed to them in the Directive.

3. Term

This Data Processing Amendment shall automatically terminate upon the expiry or termination of the Agreement.

4. Data Protection Legislation

The parties agree and acknowledge that the Data Protection Legislation applies to the processing of Customer Personal Data.

5. Processing of Customer Personal Data

5.1. **Processor**. With respect to Customer Personal Data under the Agreement, the parties acknowledge and agree that Customer shall be the controller and Google shall be a processor. Customer shall comply with its obligations as a controller and Google shall comply with its obligations as a processor under the Agreement. Where a Customer Affiliate is the controller (either alone or jointly with the Customer) with respect to certain Customer Personal Data, Customer represents and warrants to Google that it is legally authorized to instruct Google and otherwise act on behalf of such Customer Affiliate in relation to the Customer Personal Data in accordance with the Agreement, as amended.

5.2 **Scope of Processing**. Google will process Customer Personal Data only in accordance with Instructions from Customer through the settings of the services, i.e. (a) to operate, maintain and support the infrastructure used to provide the Services; (b) to comply with Customer's instructions and processing instructions in their use, management and administration of the Services; (c) as otherwise instructed through settings of the Services. Google will only process Customer Personal Data in accordance with the Agreement.

5.3 **Other Services**. Customer acknowledges that if it installs, uses, or enables Additional Products that interoperate with the Services but are not part of the Services itself, then the Services may allow such Additional Products to access Customer Personal Data as required for the interoperation of those Additional Products with the Services. By using such Additional Products, Customer authorizes Google to share Customer Personal Data with the Additional Products. The Agreement does not apply to the processing of Customer Personal Data transmitted to and from such other Additional Products. Such separate Additional Products are not required to use the Services and may be restricted for use as determined by Customer's system administrator in accordance with the Agreement.

6. Data Security

6.1 **Security Measures**. Google will take and implement appropriate technical, administrative and organizational measures designed to protect Customer Personal Data against a Security Incident ("Security Measures"). As of the Effective Date Google has implemented the Security Measures in Appendix 1. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Services.

6.2 **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.

6.3 **Security Incident**. If Google becomes aware of a Security Incident, Google will notify Customer of such Security Incident as soon as reasonably practicable, having regard to the nature of such Security Incident. Google will use commercially reasonable efforts to work with Customer in good faith to address any known breach of Google's security obligations under the Agreement.

6.4 **Security Certification**. During the Term, Google will maintain its ISO/IEC 27001:2013 certification or a comparable certification for the Services.

6.5 **Distribution of Audit Certificate**. Google will review the audit certificate at least every eighteen (18) months. A copy of the audit certificate is available on Google's website.

6.6 **Audit Rights**. Google has included the security certification and audit obligations in Sections 6.4 and 6.5 of this Data Processing Amendment at the request of the Customer.

7. Data Deletion

For the term of the Agreement Google will provide Customer with the ability to export Customer Personal Data in a manner consistent with the functionality of the Services. After termination or expiry of the Google Analytics Agreement, Google will delete Customer Personal Data in accordance with the terms of the Agreement.

8. Access to Data

Google will make available to Customer the Customer Personal Data in accordance with the terms of the Agreement in a manner consistent with the functionality of the Services, including the SLA (if applicable).

9. Data Transfers

9.1 **Data Transfers**. As part of providing the Services, Google may transfer, store and process Customer Personal Data in the United States or any other country in which Google maintains facilities.

10. Subprocessors

10.1 **Subprocessors**. Google may engage Subprocessors to provide limited parts of the Services (including customer support services).

10.2 **Processing Restrictions**. Google will ensure Subprocessors only access and use Customer Personal Data in accordance with the terms of the Agreement.

10.3 **Customer Consent to Subprocessing**. Customer consents to Google subcontracting the processing of Customer Personal Data to Subprocessors in accordance with the terms of the Agreement.

11. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Google Inc. isn't a party to the Google Analytics Agreement, the applicable Google Inc. subsidiary will be a third party beneficiary of this Data Processing Amendment.

12. Effect of Amendment

To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, the Agreement remains in full force and effect.

Appendix: Security Measures

As of the Effective Date, Google abides by the Security Measures set forth this this Appendix to the Data Processing Amendment. During the term of the Agreement, the Security Measures may change but Google agrees that any such change shall not cause a material degradation in the security of the Services.

1. Data Center & Network Security

(a) Data Centers.

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

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize 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 center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center 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 center. Backup power is provided by various mechanisms such as uninterruptible power supplies (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 center, 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 center at full capacity typically for a period of days.

Server Operating Systems. Google servers use hardened operating systems customized 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. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. 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 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) available.

2. Access and Site Controls

(a) Site Controls.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center 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 center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers 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 center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that are 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. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers 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 for 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 employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys 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 minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; principle of least privilege; and must 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 centers. A central authentication system is used across all Services to increase uniform security of data.

(b) Decommissioned Disks and Data 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.

5. Subprocessor Security

Prior to 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, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Google Analytics Data Processing Amendment