Data Processing and Security Terms for AppSheet Services

Last modified: 30 June 2022

The customer agreeing to these terms ("Customer"), and Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., or any other entity that directly or indirectly controls, is controlled by, or is under common control with Google LLC (as applicable, "Google"), have entered into an agreement under which Google has agreed to provide the Services described at https://solutions.appsheet.com/application-platform and related technical support to Customer (as amended from time to time, the "Agreement").

1. Commencement

These Data Processing and Security Terms, including their appendices (the "Terms") will be effective and replace any previously applicable data processing and security terms as from the Terms Effective Date (as defined below). These Terms supplement the Agreement. Where the Agreement was entered into offline with Google Ireland Limited, these Terms supersede the "Privacy" Clause in that agreement (if applicable).

2. Definitions

2.1 Capitalized terms defined in the Agreement apply to these Terms. In addition, in these Terms:

Additional Security Controls means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including the Admin Console, logging and monitoring, and access management.

Adequate Country means:

(a) for data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR;

(b) for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or

(c) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.

Alternative Transfer Solution means a solution, other than the SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law.

Customer Data has the meaning given in the Agreement or, if no such meaning is given, means data provided to Google by Customer or Customer End Users through the Services under the Account.

Customer End User has the meaning given in the Agreement or, if no such meaning is given, has the meaning given to "End User" in the Agreement.

Customer Personal Data means the personal data contained within the Customer Data.

Customer SCCs means the SCCs (EU Controller-to-Processor), SCCs (EU Processor-to-Processor), the SCCs (EU Processor-to-Controller), and/or the SCCs (UK Controller-to-Processor), as applicable.

Data Incident means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to,

Customer Data on systems managed by or otherwise controlled by Google.
EEA means the European Economic Area.
EMEA means Europe, the Middle East and Africa.
EU GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
European Data Protection Law means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
European Law 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).
GDPR means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.
Google's Third Party Auditor means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.
Instructions has the meaning given in Section 5.2.1 (Customer's Instructions).
Non-European Data Protection Law means data protection or privacy laws in force outside the European Economic Area, Switzerland and the UK.
Notification Email Address means the email address associated with Customer's Account Customer is responsible for keeping its Notification Email Address current and valid.
SCCs means the Customer SCCs and/or SCCs (EU Processor-to-Processor, Google Exporter), as applicable.
SCCs (EU Controller-to-Processor) means the terms at:
https://appsheet.com/terms/sccs/eu-c2p
SCCs (EU Processor-to-Controller) means the terms at:
https://appsheet.com/terms/sccs/eu-p2c
SCCs (EU Processor-to-Processor) means the terms at:
https://appsheet.com/terms/sccs/eu-p2p
SCCs (EU Processor-to-Processor, Google Exporter) means the terms at:
https://appsheet.com/terms/sccs/eu-p2p-google-exporter
SCCs (UK Controller-to-Processor) means the terms at:
https://appsheet.com/terms/sccs/uk-c2p
Security Documentation means all documents and information made available by Google under Section 7.5.1 (Reviews of Security Documentation).
Security Measures has the meaning given in Section 7.1.1 (Google's Security Measures).
Subprocessor means a third party authorized as another processor under these Terms to have logical access to and process Customer Data in order to provide parts of the Services and TSS.
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.
Swiss FDPA means the Federal Data Protection Act of 19 June 1992 (Switzerland).
Term means the period from the Terms Effective Date until the end of Google's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.
Terms Effective Date means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.
UK GDPR means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

2.2 The terms "personal data", "data subject", "processing", "controller" and "processor" as used in these Terms have the meanings given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

3. Duration

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

4. Scope of Data Protection Law

4.1 Application of European Law. The parties acknowledge that European Data Protection Law will apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or
b. the 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 in the EEA or the UK, or the monitoring of their behavior in the EEA or the UK.

4.2 Application of Non-European Law. The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.

4.3 Application of Terms. Except to the extent these Terms state otherwise, these Terms will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

5. Processing of Data

5.1 Roles and Regulatory Compliance; Authorization.

5.1.1 Processor and Controller Responsibilities. If European Data Protection Law applies to the processing of Customer Personal Data:

a. the subject matter and details of the processing are described in Appendix 1;
b. Google is a processor of that Customer Personal Data under European Data Protection Law;
c. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and
d. each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.

5.1.2 Processor Customers. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor:

a. Customer warrants on an ongoing basis that the relevant controller has authorized: (i) the Instructions, (ii) Customer's appointment of Google as another processor, and (iii) Google's engagement of Subprocessors as described in Section 11 (Subprocessors);
b. Customer will immediately forward to the relevant controller any notice provided by Google under Sections 5.2.3 (Instruction Notifications), 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), 11.4 (Opportunity to Object to Subprocessor Changes) or that refers to any SCCs; and
c. Customer may:
    i. request access for the relevant controller to the SOC Reports in accordance with Section 7.5.3(a); and
    ii. make available to the relevant controller any other information made available by Google under Sections 10.4 (Supplementary Measures and Information), 10.6 (Data Center Information) and 11.2 (Information about Subprocessors).

5.1.3 Responsibilities under Non-European Law. If Non-European Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations

applicable to it under that law with respect to the processing of that Customer Personal Data.

5.2 Scope of Processing.

5.2.1 Customer's Instructions. Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and TSS; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement, including these 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 Terms (collectively, the "Instructions").

5.2.2 Google's Compliance with Instructions. Google will comply with the Instructions unless prohibited by European Law.

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

6. Data Deletion

6.1 Deletion by Customer. Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an instruction to Google to delete the relevant Customer Data 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 European Law requires storage.

6.2 Deletion on Termination. On expiry of the Term, Customer instructs Google to delete all Customer 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 European Law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer is responsible for exporting, before the Term expires, any Customer Data it wishes to retain.

7. Data Security

7.1 Google's Security Measures, Controls and Assistance.

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

7.1.2 Access and Compliance. Google will: (a) authorize its employees, contractors and Subprocessors to access Customer Personal Data only as strictly necessary to comply with Instructions; (b) 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, and (c) ensure that all persons authorized to process Customer Personal Data are under an obligation

of confidentiality.

7.1.3 Additional Security Controls. Google will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4 Google's Security Assistance. 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 its obligations pursuant to Articles 32 to 34 of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);
b. making Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);
c. complying with the terms of Section 7.2 (Data Incidents);
d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the Agreement including these Terms; and
e. if subsections (a)-(d) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

7.2 Data Incidents.

7.2.1 Incident Notification. Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Google's notification of a Data Incident will describe, to the extent possible, the nature of the Data Incident, the measures taken to mitigate the potential risks and the measures Google recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address.

7.2.4 No Assessment of Customer Data by Google. Google has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

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. Without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Google's or Google's Subprocessors' systems, including:

a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;
b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and
c. backing up its Customer Data as appropriate.

7.3.2 Customer's Security Assessment. Customer agrees, based on its current and intended use of the Services, that the Services, Security Measures, Additional Security Controls and Google's commitments under this Section 7 (Data Security): (a) meet Customer's needs, including with respect to any security obligations of Customer under European Data Protection Law and/or Non-European Data Protection Law, as applicable, and (b) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4 SOC Report. Google will maintain at least the following for the Services in order to evaluate the continued effectiveness of the Security Measures: a SOC 2 report produced by Google's Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the "SOC Report"). Google may add standards at any time. Google may replace a SOC Report with an equivalent or enhanced alternative.

7.5 Reviews and Audits of Compliance.

7.5.1 Reviews of Security Documentation. Google will make the SOC Report available for review by Customer to demonstrate compliance by Google with its obligations under these Terms.

7.5.2 Customer's Audit Rights.

a. If European Data Protection Law applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under these Terms in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Google will contribute to such audits as described in Section 7.4 (SOC Report) and this Section 7.5 (Reviews and Audits of Compliance).
b. If Customer SCCs apply as described in Section 10.3 (Restricted Transfers), Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).
c. Customer may conduct an audit to verify Google's compliance with its obligations under these Terms by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third Party Auditor).

7.5.3 Additional Business Terms for Reviews and Audits.

a. Customer must send any requests for reviews of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1 or audits under Section 7.5.2(a) or 7.5.2(b) to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).
b. Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) or 7.5.2(b).
c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) or 7.5.2(b). 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 auditor appointed by Customer to execute any such audit.
d. Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) or 7.5.2(b) 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.

8. Impact Assessments and Consultations

Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with its obligations pursuant to Articles 35 and 36 of the GDPR, by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation);
b. providing the information contained in the Agreement (including these Terms); and
c. if subsections (a) and (b) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

9. Access etc.; Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by applicable European Data Protection Law.

9.2 Data Subject Requests.

9.2.1 Responsibility for Requests. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject in relation to Customer Personal Data, and the request identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Google's Data Subject Request Assistance. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);
b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and
c. if subsections (a) and (b) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

10. Data Transfers

10.1 Data Storage and Processing Facilities. Subject to the remainder of this Section 10 (Data Transfers), Customer Data may be processed in any country in which Google or its Subprocessors maintain facilities.

10.2 Permitted Transfers. The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country ("Permitted Transfers").

10.3 Restricted Transfers. If the processing of Customer Personal Data involves any transfers that are not Permitted Transfers, and European Data Protection Law applies to those transfers if its billing address is outside EMEA) ("Restricted Transfers"), then:

a. if Google announces its adoption of an Alternative Transfer Solution for any Restricted Transfers, then Google will ensure that they are made in accordance with that Alternative Transfer Solution; and/or
b. if Google has not adopted an Alternative Transfer Solution for any Restricted Transfers, then:
    i. if Google's address is in an Adequate Country:
        A. the SCCs (EU Processor-to-Processor, Google Exporter) will apply with respect to all Restricted Transfers from Google to Subprocessors; and
        B. in addition, if Customer's billing address is not in an Adequate Country, the SCCs (EU Processor-to-Controller) will apply (regardless of whether Customer is a controller and/or processor) with respect to Restricted Transfers between Google and Customer; or
    ii. if Google's address is not in an Adequate Country:
        A. the SCCs (EU Controller-to-Processor) and/or SCCs (EU Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to Restricted Transfers between Customer and Google that are subject to the EU GDPR and/or the Swiss FDPA; and
        B. the SCCs (UK Controller-to-Processor) will apply (regardless of whether Customer is a controller and/or processor) with respect to Restricted Transfers between Customer and Google that are subject to the UK GDPR.

10.4 Supplementary Measures and Information. Google may provide Customer with information relevant to Restricted Transfers, including information about Additional Security Controls and other supplementary measures to protect Customer Personal Data as described in Section 7.5.1 (Reviews of Security Documentation).

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

10.6 Data Center Information. Information about the locations of Google facilities is available at: https://cloud.google.com/about/locations/ (as may be updated by Google from time to time).

11. Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Terms Effective Date at the URL specified in Section 11.2 (Information about Subprocessors); and (b) all other Google Affiliates from time to time. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement as Subprocessors of any other third parties ("New Subprocessors").

11.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at: https://cloud.google.com/terms/subprocessors and https://solutions.appsheet.com/gdpr-compliance (as may be updated by Google from time to time in accordance with these Terms).

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 Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Terms) ; and
ii. if the processing of Customer Personal Data is subject to European Data Protection Law, the data protection obligations described in these Terms (as referred to in Article 28(3) of the GDPR, if applicable), 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 Subprocessor is engaged during the Term, Google will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform).

b. Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by terminating the Agreement immediately by notifying Google.

12. Cloud Data Protection Team; Processing Records

12.1 Google's Cloud Data Protection Team. Google's Cloud Data Protection Team for the Services will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Personal Data under the Agreement and can be contacted at support@appsheet.com (and/or via such other means as Google may provide from time to time).

12.2 Google's Processing Records. Google will keep appropriate documentation of its processing activities as required by the GDPR. To the extent the GDPR requires Google to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information and keep it accurate and up-to-date. Google may make any such information available to the Supervisory Authorities if required by the GDPR.

12.3 Controller Requests. During the Term, if Google's Cloud Data Protection Team receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Google will advise the third party to contact Customer.

13. Interpretation

13.1 Precedence. To the extent of any conflict or inconsistency between:

a. these Terms and the remainder of the Agreement, these Terms will prevail; and
b. any Customer SCCs (which are incorporated by reference into these Terms) and the remainder of the Agreement (including these Terms), the Customer SCCs will prevail.

13.2 Legacy MCCs. The SCCs will, as of the Transition Date, supersede and terminate any Model Contract Clauses approved under Directive 95/46/EC and previously entered into by Customer and Google LLC. The "Transition Date" means 27 September 2021. Where Google LLC is not a party to the Agreement, Google LLC will be a third party beneficiary of this Section 13.2.

13.3 No Modification of SCCs. Nothing in the Agreement (including these Terms) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter
Google's provision of the Services and TSS to Customer.

Duration of the Processing

The Term plus the period from the expiry of the Term until deletion of all Customer Data by Google in accordance with the Terms.

Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with the Terms.

Categories of Data

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or by Customer End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or by Customer End Users.

Appendix 2: Security Measures

As from the Terms Effective Date, Google will implement and maintain the Security Measures described in this Appendix 2.

1. Data Center and 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, 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 a Linux based implementation customized for the application environment. 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 has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization 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 minimize the impact of a compromised key, or a cryptographic breakthrough.

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 require 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; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ a dual authentication 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. 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 up to 30 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 must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. 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. Google's authentication and authorization systems utilize SSH certificates and security keys, and 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; 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. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.

3. Data

(a) Data Storage, Isolation and Logging. Google stores data in a multi-tenant environment on Google-

owned servers. Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates the Customer's data. Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to Customer End Users for specific purposes. Customer may choose to make use of logging functionality that Google makes available via the Services.

(b) Decommissioned Disks and Disk Erase Policy. 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 "Disk Erase Policy") 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 Disk Erase Policy.

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 Data are required to complete additional requirements appropriate to their role (e.g., certifications). Google's personnel will not process Customer Data without authorization.

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 to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement) of these Terms, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.