Data Processing and Security Terms for Apigee Products (v 1.0)

Customer and Google (as defined in the Google General Terms and Conditions for Apigee Products) have entered into Google General Terms and Conditions for Apigee Products (as amended to date, the "General Terms"). These Data Processing and Security Terms for Apigee Products, including the Appendices (collectively, the “Security Terms”) are entered into by Customer and Google as of the effective date of the General Terms (“Terms Effective Date”) and supplement the General Terms. These Security Terms supersede any data processing and security terms entered into between Customer and Google on the same subject matter, and may be updated from time to time in accordance with the General Terms

1. Introduction

These Security Terms reflect the parties’ agreement with respect to terms governing the processing of Customer Personal Data under the General Terms.

2. Definitions

2.1 Capitalized terms used but not defined in these Security Terms have the meanings set out in the General Terms. In these Security Terms, 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 Cloud Services, but that may be accessible via the Admin Console or otherwise, for use with the Cloud Services.
- Agreement means the General Terms, as supplemented by these Security Terms, and as may be further amended from time to time in accordance with the General Terms.
- Alternative Transfer Solution means any solution, other than the Model Contract Clauses, that ensures an adequate level of protection of personal data in a third country within the meaning of Article 25 of the Directive.
- Customer Personal Data means the personal data that is contained within the Customer Data.
- Data Incident means (a) any unlawful access to Customer Data stored in the Cloud Services or systems, equipment, or facilities of Google or its Subprocessors, or (b) unauthorized access to such Cloud Services, systems, equipment, or facilities that results in loss, disclosure, or alteration of Customer Data.
- Data Protection Legislation means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Customer and/or any Customer Affiliates as the controller(s) of the Customer Personal Data; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
- 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.
- EEA means the European Economic Area.
- Google Group means those Google Affiliates involved in provision of the Cloud Services to Customer.
- Instructions means Customer’s written instructions to Google consisting of the Agreement, including instructions to Google to provide the Cloud Services as set out in the Agreement; instructions given by Customer via the Admin Console and otherwise in

its use of the Cloud Services; and any subsequent written instructions given by Customer to Google and acknowledged by Google.

- Model Contract Clauses or MCCs mean the standard contractual clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
- Security Measures has the meaning given in Section 6.1 (Security Measures) of these Security Terms.
- Subprocessors means (a) all Google Group entities that have logical access to, and process, Customer Personal Data (each, a "Google Group Subprocessor"), and (b) all third parties (other than Google Group entities) that are engaged to provide services to Customer and that have logical access to, and process, Customer Personal Data (each, a "Third Party Subprocessor").
- Third Party Auditor means a qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

2.2 The terms "personal data", "processing", "data subject", "controller" and "processor" have the meanings given to them in the Directive. The terms "data importer" and "data exporter" have the meanings given to them in the Model Contract Clauses.

3. Term

These Security Terms will take effect on the Terms Effective Date and, notwithstanding expiry or termination of the General Terms, will remain in effect until, and automatically terminate upon, deletion by Google of all data as described in Section 7 (Data Correction, Blocking, Exporting, and Deletion) of these Security Terms.

4. Data Protection Legislation

The parties agree and acknowledge that the Data Protection Legislation will apply to the processing of Customer Personal Data if, for example, the processing is carried out in the context of the activities of an establishment of the Customer (or of an authorized Customer Affiliate) in the territory of an EU member state.

5. Processing of Customer Personal Data

5.1 Controller and Processor. If the Data Protection Legislation applies to the processing of Customer Personal Data, then as between the parties, the parties acknowledge and agree that: (a) Customer is the controller of Customer Personal Data under the Agreement; (b) Google is a processor of such data; (c) Customer will comply with its obligations as a controller under the Data Protection Legislation; and (d) Google will comply with its obligations as a processor under the Agreement. If under the Data Protection Legislation a Customer Affiliate is considered the controller (either alone or jointly with the Customer) with respect to certain Customer Personal Data, Customer represents and warrants to Google that Customer is authorized: (i) to give the Instructions to Google and otherwise act on behalf of such Customer Affiliate in relation to such Customer Personal Data as described in these Terms, and (ii) to bind the Customer Affiliate to these Security Terms. Appendix 1 sets out a description of the categories of data that may fall within Customer Personal Data and of the categories of data subjects to which that data may relate.

5.2 Scope of Processing.Google will only process Customer Personal Data in accordance with the Instructions, and will not process Customer Personal Data for any other purpose.

5.3 Additional Products. Customer acknowledges that if it installs, uses, or enables Additional Products, then the Cloud Services may allow such Additional Products to access Customer Data as required for the interoperation of those Additional Products with the Cloud Services. The Agreement does not apply to the processing of data transmitted to or from such Additional Products. Such Additional Products are not required to use the Cloud Services.

6. Data Security; Security Compliance; Audits

6.1 Security Measures. Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration, or unauthorized disclosure or access, or other unauthorized processing, as detailed in Appendix 2 (the "Security Measures"). 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 Cloud Services. Customer agrees that it is solely responsible for its use of the Cloud Services, including securing its account authentication credentials, and that Google has no obligation to protect Customer Data that Customer elects to store or transfer outside of Google's systems (e.g., offline or on-premise storage).

6.2 Security Compliance by Google Staff. Google will take appropriate steps to ensure compliance with the Security Measures by its employees and contractors to the extent applicable to their scope of performance.

6.3 Data Incidents. If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the email address provided by Customer in the Agreement (or in the Admin Console) or, at Google's discretion, by direct Customer communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring that the contact information set forth above is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Cloud Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

6.4 SOC 2 Reports. During the Term, Google will maintain its confidential Service Organization Control (SOC) 2 report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability applicable to the Cloud Services ("SOC 2 Report"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months.

6.5 Auditing Security Compliance.

6.5.1 Reviews of Security Documentation. Google will make the following available for review by Customer: (a) a summary or redacted version of the then-current confidential SOC 2 Report; and (b) following a request by Customer in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.

6.5.2 Customer Audits. If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 of these Terms, Customer or such Customer Affiliate may exercise the audit rights granted under clauses 5(f) and 12(2) of such Model Contract Clauses: (a) by instructing Google to execute the audit as described in Sections 6.4 and 6.5.1 above; and/or (b) following a request by Customer in accordance with Section 6.5.4 below, by executing an audit as described in such Model Contract Clauses.

6.5.3 Additional Business Terms for Reviews and Audits. Google and Customer (or an authorised Customer Affiliate if applicable) will discuss and agree in advance on: (a) the reasonable date(s) of and security and confidentiality controls applicable to any Customer review under Section 6.5.1(b); and (b) the identity of a suitably qualified independent auditor for any audit under Section 6.5.2(b), and the reasonable start date, scope and duration of and security and confidentiality controls applicable to any such audit. Google reserves the right to charge a fee (based on Google's reasonable costs) for any review under Section 6.5.1(b) and/or audit under Section 6.5.2(b). Google will provide further details of any applicable fee, and the basis of its calculation, to Customer (or an authorized Customer Affiliate), in advance of any such review or audit. For clarity, Google is not responsible for any costs incurred or fees charged by any third party auditor appointed by Customer (or an authorised Customer Affiliate) in connection with an audit under Section 6.5.2(b).

Nothing in this Section 6.5 varies or modifies any rights or obligations of Customer (or any authorized Customer Affiliate) or Google LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA) of these Security Terms.

6.5.4 Requests for Reviews and Audits. Any requests under Section 6.5.1 or 6.5.2 must be sent to the Data Privacy Office as described in Section 9 (Data Privacy Office) of these Security Terms.

7. Data Correction, Blocking, Exporting, and Deletion

During the Term of the Cloud Services, Google will provide Customer with the ability to correct, block, export and delete Customer Data in a manner consistent with the functionality of the Cloud Services and in accordance with the terms of the Agreement. On the expiry or termination of the Agreement (or, if applicable on expiry of any post-termination period during which Google may agree to continue providing access to the Cloud Services), Google may thereafter delete Customer Data, unless applicable legislation or legal process prevents it from doing so.

8. Access; Export of Data

During the Term of the Cloud Services, Google will make available to Customer the Customer Data in a manner consistent with the functionality of the Cloud Services and in accordance with the terms of the Agreement. To the extent Customer, in its use and administration of the Cloud Services during the Term, does not have the ability to amend or delete Customer Data (as required by applicable law), or migrate Customer Data to another system or service provider, Google will, at Customer's reasonable expense, comply with any reasonable requests from Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the relevant Customer Data.

9. Data Privacy Office

Google's Data Privacy Office can be contacted by Customer administrators at: enterprise-dpo@google.com (or via such other means as Google may provide).

10. Data Transfers

10.1 Data Location and Transfers. Customer may select where certain Customer Data will be stored (the "Data Location Setting"), and Google will store it there in accordance with the General Terms. If a Data Location Setting is not covered by the General Terms (or a Data Location Setting is not made by Customer in respect of any Customer Data), Google may store and process the relevant Customer Data anywhere Google or its Subprocessors maintain facilities.

10.2 Transfers of Data Out of the EEA.

10.2.1 Customer Obligations. If the storage and/or processing of Customer Data (as set out in Section 10.1 above) involves transfers of Customer Personal Data out of the EEA, and Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), Customer acknowledges that Data Protection Legislation will require Customer (or an authorized Customer Affiliate) to enter into Model Contract Clauses in respect of such transfers, unless Google has adopted an Alternative Transfer Solution.

10.2.2 Google Obligations. In respect of Transferred Personal Data, Google will: (a) if requested to do so by Customer, ensure that Google LLC as the data importer of the Transferred Personal Data enters into Model Contract Clauses with Customer (or an authorized Customer Affiliate) as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or (b) adopt an Alternative Transfer Solution, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available about its adoption of such solution.

10.3 Data Center Information. Google will make available to Customer information about the countries in which data centers used to store Customer Personal Data are located.

10.4 Disclosure of Confidential Information Containing Personal Data. If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Google will, notwithstanding any term to the contrary in the Agreement, ensure that any disclosure of Customer's (or, if applicable, an authorized Customer Affiliate's) Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. Consent to Subprocessing

11.1 Consent to Subprocessing. If Model Contract Clauses have been entered into by Google LLC and Customer (or an authorized Customer Affiliate), Customer (or, if applicable, an authorized Customer Affiliate): (a) consents to Google LLC subcontracting the processing of Customer Data in accordance with the terms of the Model Contract Clauses; and (b) acknowledges that this constitutes the prior written consent of Customer (or the applicable authorized Customer Affiliate) for the purpose of clause 11(1) of the Model Contract Clauses.

11.2 Termination. If the Model Contract Clauses have been entered into by the parties: (a) Google will, at least 15 days before appointing any new Third Party Subprocessor, inform Customer of the appointment (including the name and location of such Subprocessor and the activities it will perform); and (b) if Customer objects to Google's use of any new Third Party Subprocessors, Customer may, as its sole and exclusive remedy, terminate the General Terms by giving written notice to Google within 30 days of being informed by Google of the appointment of such Subprocessor.

12. Liability Cap

If Google LLC and Customer (or an authorized Customer Affiliate) enter into Model Contract Clauses as described above, then, subject to the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability), the total combined liability of Google and its Affiliates towards Customer and its Affiliates, on the one hand, and Customer and its Affiliates towards Google and its Affiliates, on the other hand, under or in connection with the Agreement and all those MCCs combined will be limited to the maximum monetary or payment-based liability amount set out in the Agreement.

13. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Google LLC is not a party to the Agreement, Google LCC will be a third party beneficiary of Section 6.5 (Auditing Security Compliance), Section 11.1 (Consent to Subprocessing), and Section 12 (Liability Cap) of these Terms.

14. Priority

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between these Security Terms and the remaining terms of the Agreement, these Security Terms will govern.

Appendix 1: Categories of Personal Data and Data Subjects

1 Categories of Personal Data. Data relating to individuals provided to Google via the Cloud Services by (or at the direction of) Customer.

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

Appendix 2: Security Measures

As of the Terms Effective Date, Google will take and implement the Security Measures set out in this Appendix. 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 Cloud Services.

1. Data Center and Network Security

This Section describes only Google owned and operated data center and network security and not those of Third Party Subprocessors.

(a) Google 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 Cloud 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. 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 Cloud 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) Google 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.
- 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.

2. Access and Site Controls

(a) Site Controls. This Section describes only Google owned and operated data center site controls and not those of Third Party Subprocessors.

- 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; 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 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. 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 Cloud Services, and responding to security incidents.
- Access Control and Privilege Management. Customer's administrators must authenticate themselves via a username and password or via a single sign on system in order to administer the Cloud 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 policies only permit authorized persons to access data they are authorized to access. 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. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented.

3. Data

- (a) Data Storage, Isolation and Logging. Google stores data in a multi-tenant environment. The data and file system architecture are replicated between multiple geographically dispersed data

centers. Google also logically isolates the Customer's data. The Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Cloud Services, will enable Customer to determine the product sharing settings applicable to individuals Customer permits to use the Cloud Services for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services.

- (b) Decommissioned Disks and Disk Erase Policy in Google Data Centers. 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 "Disk Erase Policy") before leaving Google owned and operated data centers 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 (eg., certifications). Google's personnel will not process Customer Data without authorization.

5. Amazon Web Services Security

Google uses data center services provided Amazon Web Services ("AWS") for the delivery of the Cloud Services and Customer acknowledges that the current AWS security features and processes are described at http://aws.amazon.com/security/. Each year, Google will review and evaluate the applicable third party security audit reports provided by AWS for environmental and physical security controls.