Data Processing and Security Terms

1. Introduction

These Data Processing and Security Terms, including the Appendices (collectively, the "Terms") supplement the Agreement. These Terms reflect the parties' agreement with respect to terms governing the processing of Partner Personal Data under the Agreement.

2. Definitions

2.1 In these 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 Services, but that may be accessible via the Admin Console or otherwise, for use with the Services.

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

Data Incident means (a) any unlawful access to Partner Data stored in the Services or systems, equipment, or facilities of Google or its Subprocessors, or (b) unauthorized access to such Services, systems, equipment, or facilities that results in loss, disclosure, or alteration of Partner Data.

Data Protection Legislation means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Partner and/or any Customers as the controller(s) of the Partner 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 Services to Partner.

Instructions means Partner's written instructions to Google consisting of the Agreement, including instructions to Google to provide the Services as set out in the Agreement; instructions given via the Admin Console and otherwise under Partner's Account; and any subsequent written instructions given by Partner (acting on behalf of itself and its Customers) to Google and acknowledged by Google.

Model Contract Clauses or MCCs mean an agreement containing 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.
Partner Personal Data means the personal data that is contained within the Partner Data.

Security Measures has the meaning given in Section 6.1 (Security Measures) of these Terms.

Subprocessors means (a) all Google Group entities that have logical access to, and process, Partner Personal Data (each, a “Google Group Subprocessor”), and (b) all third parties (other than Google Group entities) that are engaged to provide services to Partner and that have logical access to, and process, Partner 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 Partner.

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 Terms will take effect on the Terms Effective Date and, notwithstanding expiry or termination of the Agreement, 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 Terms.

4. Data Protection Legislation

The parties agree and acknowledge that the Data Protection Legislation will apply to the processing of Partner Personal Data if, for example, the processing is carried out in the context of the activities of an establishment of the Partner in the territory of an EU Member State.

5. Processing of Partner Personal Data

5.1 Controller and Processor. If the Data Protection Legislation applies to the processing of Partner Personal Data, then as between the parties, the parties acknowledge and agree that:

(a) Google will be a processor of the Partner Personal Data and will, within the scope of the Agreement, comply with its obligations as a processor under the Agreement; and

(b) where Partner is a controller with respect to certain Partner Personal Data it will, within the scope of the Agreement, comply with its obligations as a controller under the Data Protection Legislation in respect of that Partner Personal Data.

5.2 Customers. Where Partner is not the controller of certain Partner Personal Data, Partner represents and warrants to Google that:

(a) it is authorized to provide the Instructions, and otherwise act on behalf of the applicable controller, in relation to that Partner Personal Data; and

(b) Google's processing of the Partner Personal Data, in accordance with the Instructions, will not breach the Data Protection Legislation.

Appendix 1 sets out a description of the categories of data that may fall within Partner Personal Data and of the categories of data subjects to which that data may relate.

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

5.3 Additional Products. Partner acknowledges that if Additional Products are installed, used or enabled via the Admin Console or otherwise under the Partner's Account, then the Services may allow such Additional Products to access Partner Data as required for the interoperation of those Additional Products with the 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 Services.

6. Data Security; Security Compliance; Audits

6.1 Security Measures. Google will take and implement appropriate technical and organizational measures to protect Partner 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 Services. Partner agrees that it is solely responsible for its and its Customers' use of the Services, including securing its and their account authentication credentials, and that Google has no obligation to protect Partner Data that Partner or its Customers elect to store or transfer outside of Google's and its Subprocessors' 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, contractors and Subprocessors 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 Partner of the Data Incident, and take reasonable steps to minimize harm and secure Partner Data. Notification(s) of any Data Incident(s) will be delivered to the email address provided by Partner in the Agreement (or in the Admin Console) or, at Google's discretion, by direct Partner communication (e.g., by phone call or an in-person meeting). Partner 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. Partner agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Partner 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 Partner Data caused by Partner's or its Customers' use of the Services or Partner's or its Customers' 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 Compliance with Security and Privacy Standards; SOC 2 and 3 Reports. During the Term, Google will maintain the following:

(a) its ISO/IEC 27001:2013 Certification or a comparable certification for the following Services: Google App Engine, Google Compute Engine, Google Cloud Storage, Google Cloud Datastore, Google BigQuery Service, Google Cloud SQL, and Google Genomics ("ISO 27001 Certification");

(b) 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 following

Services: Google App Engine, Google Compute Engine, Google Cloud Storage, Google Cloud Datastore, Google BigQuery Service and
Google Cloud SQL (“SOC 2 Report”), as produced by the Third Party Auditor and updated at least once every eighteen (18) months; and

(c) its Service Organization Control (SOC) 3 report (or a comparable report) applicable to the following Services: Google App Engine, Google Compute Engine, Google Cloud Storage, Google Cloud Datastore, Google BigQuery Service and Google Cloud SQL (“SOC 3 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 Partner:

(a) the certificate issued in relation to Google’s ISO 27001 Certification;

(b) the then-current SOC 3 Report;

(c) a summary or redacted version of the then-current confidential SOC 2 Report; and

(d) following a request by Partner in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.

6.5.2 Partner Audits. If Partner has entered into Model Contract Clauses as described in Section 10.2 of these Terms, Partner 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 Partner 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 Partner will discuss and agree in advance on:

(a) the reasonable date(s) of and security and confidentiality controls applicable to any Partner review under Section 6.5.1(d); 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(d) and/or audit under Section 6.5.2(b). For clarity, Google is not responsible for any costs incurred or fees charged by any third party auditor appointed by Partner 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 Partner or Google Inc. under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA) of these 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 for Google Cloud Platform) of these Terms.

7. Data Correction, Blocking, Exporting, and Deletion

During the Term, Google will provide Partner with the ability to correct, block, export and delete the Partner Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Partner deletes
Partner Data via the Services such that the Partner Data cannot be recovered by Partner (the "Partner-Deleted Data"), Google will delete the Partner-Deleted Data within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so. 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 Services), after a recovery period of up to 30 days following such expiry or termination, Google will thereafter delete the PartnerDeleted Data within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

8. Access; Export of Data

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

9. Data Privacy Office for Google Cloud Platform

Google's Data Privacy Office for Google Cloud Platform can be contacted by Partner administrators at: https://support.google.com/cloud/contact/dpo (or via such other means as Google may provide).

10. Data Transfers

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

10.2 Transfers of Data Out of the EEA.

10.2.1 Partner Obligations. If the storage and/or processing of Partner Data (as set out in Section 10.1 above) involves transfers of Partner Personal Data out of the EEA, and Data Protection Legislation applies to the transfers of such data (**"Transferred Personal Data"**), Partner acknowledges that Data Protection Legislation will require Partner 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 Partner, ensure that Google Inc. as the importer of the Transferred Personal Data enters into Model Contract Clauses with Partner as the 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 and ensure that the transfers are made in accordance with such solution.

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

11. Subprocessors

11.1 Subprocessors. Google may engage Subprocessors to provide limited parts of the Services, subject to the restrictions in these Terms.

11.2 Subprocessing Restrictions. Google will ensure that Subprocessors only access and use Partner Data in accordance with Section 10.1 (Data Location and Transfers) and terms of the Agreement and that they are bound by written agreements that require them to provide at least the level of data protection required by the following, as applicable pursuant to Section 10.2 (Transfers of Data Out of the EEA): (a) any Model Contract Clauses entered into by Google Inc. and Partner; and/or (b) any Alternative Transfer Solution adopted by Google.

11.3 Consent to Subprocessing. Partner consents to Google subcontracting the processing of Partner Data to Subprocessors in accordance with the Agreement. If the Model Contract Clauses have been entered into as described above, Partner consents to Google Inc. subcontracting the processing of Partner Data in accordance with the terms of the Model Contract Clauses.

11.4 Additional Information. Information about Third Party Subprocessors is available at: https://cloud.google.com/terms/third-party-suppliers, as such URL may be updated by Google from time to time. The information available at this URL is accurate as at the time of publication. At the written request of the Partner, Google will provide additional information regarding Subprocessors and their locations. Any such requests must be sent to Google's Data Privacy Office for Google Cloud Platform, the contact details of which are set out in Section 9 (Data Privacy Office for Google Cloud Platform) above.

11.5 Termination. If the Model Contract Clauses have been entered into by the parties: (i) Google will, at least 15 days before appointing any new Third Party Subprocessor, inform Partner of the appointment (including the name and location of such subprocessor and the activities it will perform) either by sending an email to Partner or via the Admin Console; and (ii) if Partner objects to Google's use of any new Third Party Subprocessors, Partner may, as its sole and exclusive remedy, terminate the Agreement 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 Inc. and Partner 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, on the one hand, and Partner 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

13.1 Google Inc. Notwithstanding anything to the contrary in the Agreement, where Google Inc. is not a party to the Agreement, Google Inc. will be a third party beneficiary of Section 6.5 (Auditing Security Compliance), Section 11.3 (Consent to Subprocessing), and Section 12 (Liability Cap) of these Terms.

13.2 Other Third Parties. Except as expressly provided herein and subject to Section 13.1, no one other than a party to this Agreement shall have any right to enforce any of its terms. For the avoidance of doubt, this includes Customers, who shall not have any right to enforce this Agreement.

14. Priority

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between these Terms and the remaining terms of the Agreement, these 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 Services, by (or at the direction of) Partner.

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

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 Services.

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. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks 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 intrusion detection involves:

(i) tightly controlling the size and make-up of Google's attack surface through preventative measures;

(ii) employing intelligent detection controls at data entry points; and

(iii) employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents. Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) 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; 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 Services, and responding to security incidents.

Access Control and Privilege Management. Partner'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. 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; 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 password expiry, 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. The data and file system architecture are replicated between multiple geographically dispersed data centers. Google also logically isolates the Partner's data. Partner will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Partner to determine the product sharing settings applicable to Partner End Users for specific purposes. Partner may choose to make use of certain logging capability that Google may make available via the Services.

(b) Decommissioned Disks and Disk Erase Policy. 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'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 Partner Data are required to complete additional requirements appropriate to their role (eg., certifications). Google’s personnel will not process Partner Data without authorization.

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, then subject to the requirements set out in Section 11.2 (Subprocessing Restrictions) of these Terms, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.