Google Apps

Data Processing Amendment to Google Apps Agreement

The Customer agreeing to these terms (“**Customer**”) and Google Inc., Google Ireland Limited, or Google Asia Pacific Pte. Ltd. (as applicable, “**Google**”) have entered into a Google Apps Enterprise Agreement, Google Apps for Business Agreement, Google Apps Enterprise via Reseller Agreement, Google Apps for Business via Reseller Agreement, Google Apps for Education Agreement, or Google Apps for Education via Reseller Agreement, as applicable, (as amended to date, the "**Google Apps Agreement**"). This amendment (the “**Data Processing Amendment**”) is entered into by Customer and Google as of the Amendment Effective Date and amends the Google Apps Agreement. The “**Amendment Effective Date**” is the date Customer accepts this Data Processing Amendment by clicking to accept these terms.

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

1. **Introduction**.

   This Data Processing Amendment reflects the parties’ agreement with respect to terms governing the processing of Customer Data under the Google Apps Agreement.

2. **Definitions**.

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

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

   “**Advertising**” means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using the "Google Sites" functionality within the Services).

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

   “**Agreement**” means the Google Apps Agreement and this Data Processing Amendment.

   “**Customer Data**” means data (which may include personal data and the categories of data referred to in Appendix 1) submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

   “**Data Protection Legislation**” means the national provisions adopted pursuant to the Directive, applicable to the Customer and the Customer Affiliates (if applicable) as the controller of the Customer Data and the Federal Data Protection Act of 19 June 1992 (Switzerland), as applicable.

   “**Directive**” means Directive 95/46/EC of the European Parliament and of the Council on the

Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

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

“**Instructions**” means instructions provided by Customer via the Admin Console, instructions initiated by the Customer and End Users in their use of the Services, the written instructions of the Customer specified in this Agreement (as amended or replaced) and any subsequent written instructions from the Customer to Google and acknowledged by Google.

“**Model Contract Clauses**” means 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.

“**Safe Harbor Privacy Principles**” means the U.S. Department of Commerce Safe Harbor framework requirements as set out at the following URL: http://export.gov/safeharbor/eu/eg_main_018475.asp, or any replacement framework or URL from time to time.

“**Security Incident**” means accidental or unlawful distribution or accidental loss, alteration, or unauthorised disclosure or access to Customer Data by Google, its Subprocessors or any third party, provided that such incident is not directly or indirectly caused by Customer’s or End User’s act or omission.

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

“**Subprocessors**” means those members of the Google Group and Third Party Suppliers that have logical access to, and process, Customer Data.

“**Services**” means

(a) for purposes of this Data Processing Amendment, those services defined as the “Google Apps Core Services” (including updates and upgrades to such Services) under the Agreement which are more fully described at the following URL: www.google.com/apps/intl/en/terms/user_features.html, as such URL may be updated from time to time by Google; and

(b) for purposes of all provisions of this Data Processing Amendment except Sections 6.4, 6.5, 6.6 and 6.7, Google Classroom as more fully described at the above-mentioned URL.

“**Third Party Suppliers**” means the third party suppliers engaged by the Google Group for the purposes of processing Customer Data in the context of the provision of the Services. Additional information about Third Party Suppliers is available at the following URL: www.google.com/intl/en/work/apps/terms/subprocessors.html, as such URL may be updated from time to time by Google. The information available at the URL is accurate at the time of publication.

2.2. The terms “personal data”, “processing”, “controller” and “processor” will have the meanings ascribed to them in the Directive.

3. **Term**.

This Data Processing Amendment will automatically terminate upon the expiry or termination of the Google Apps Agreement.

4. **Data Protection Legislation**.

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

5. **Processing of Customer Data**.

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

5.2. **Scope of Processing**. Google will process Customer Data in accordance with Customer’s Instructions. Customer instructs Google to process Customer Data to: (i) provide the Services (which includes the detection, prevention and resolution of security and technical issues) and (ii) respond to customer support requests.

5.3. **Processing Restrictions**. Google will only process Customer Data in accordance with this Agreement and will not process Customer Data for any other purpose. For clarity, and notwithstanding any other term in the Agreement, Google will not serve Advertising in the Services or use Customer Data for Advertising purposes.

5.4. **Other Services**. Customer acknowledges that if it installs, uses, or enables Additional Products that interoperate with the Services but are not part of the Services itself, then the Services may allow such Additional Products to access Customer 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 and from such other Additional Products. Such separate Additional Products are not required to use the Services and may be restricted for use as determined by Customer’s system administrator in accordance with the Agreement.

6. **Data Security**.

6.1. **Security Measures**. Google will take and implement appropriate technical, administrative and organizational measures designed to protect Customer Data against a Security Incident ("**Security Measures**"). As of the Amendment Effective Date Google has implemented the Security Measures in Appendix 2. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Services. Customer agrees that Google has no obligation to protect Customer Data that Customer elects to store outside of Google’s and its Subprocessors systems (eg., offline or on-premise storage).

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

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

6.4. **Security Certification**. During the Term, Google will maintain its ISO/IEC 27001:2005 Certification or a comparable certification (“**ISO Certification**”) for the Services.

6.5. **Security Audit**. During the Term, Google will maintain its Statement on Standards for Attestation Engagements (SSAE) No. 16 Type II / International Standards for Assurance Engagements (ISAE) No. 3402 report (or a comparable report) on Google’s systems examining logical security controls, physical security controls, and system availability (“**Audit Report**”) as related to the Services.

6.6. **Distribution of Audit Report**. Google will update the Audit Report, at least every eighteen (18) months. A summary of the Audit Report is available on Google’s website.

6.7. **Audit Rights**. Google has included the security certification and audit obligations in Sections 6.4, 6.5 and 6.6 of this Data Processing Amendment at the request of the Customer, and where Customer or a Customer Affiliate has entered into the Model Contract Clauses with a Google Group entity as described under Section 10.3 (Model Contract Clauses), Customer agrees that the security certification and audit obligations of this Data Processing Amendment will be deemed to fully satisfy the audit rights granted under clauses 5(f) and 12(2) of such Model Contract Clauses with respect to Customer and any applicable authorized Customer Affiliate.

7. **Data Correction, Blocking and Deletion**.

7.1. **Customer and End User Deletion**. For the term of the Agreement Google will provide Customer or End Users with the ability to correct, block, export and delete Customer Data in a manner consistent with the functionality of the Services. Once Customer or End User deletes Customer Data and such Customer Data cannot be recovered by the Customer or End User, such as from the “trash" (“Customer-Deleted Data”),Google will delete such Customer-Deleted Data from its systems as soon as reasonably practicable and within a maximum period of 180 days.

7.2. **Deletion on Termination**. On expiry or termination of the Google Apps Agreement, Google will delete all Customer-Deleted Data from its systems as soon as reasonably practicable and within a maximum period of 180 days.

8. **Access to Data**.

Google will make available to Customer the Customer Data in accordance with the terms of the Agreement in a manner consistent with the functionality of the Services, including the applicable SLA. To the extent Customer, in its use and administration of the Services, 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 comply with any reasonable requests by Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the Customer Data.

9. **Data Privacy Officer**.

The Data Privacy Officer for Google Apps can be contacted at: enterprise-dpo@google.com.

10. **Data Transfers**.

10.1. **Data Transfers**. As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google and its Subprocessors maintain facilities.

10.2. **Safe Harbor**. During the Term, Google will ensure that Google Inc. remains enrolled in the U.S Department of Commerce Safe Harbor Program (“Safe Harbor”) or adopts an alternative compliance solution that achieves compliance with the terms of the Directive for transfers of personal data to a third country. While Google Inc. remains enrolled in Safe Harbor: (i) the scope of Google Inc.'s Safe Harbor certification will include Customer personal data; and (ii) the Google Group’s processing practices in respect of Customer personal data will remain consistent with those described in Google Inc.'s Safe Harbor certification and the Safe Harbor Privacy Principles.

10.3. **Model Contract Clauses**. During the Term Customer (or an authorized Customer Affiliate established in the European Economic Area) may enter into Model Contract Clauses with Google Inc.

11. **Subprocessors**.

11.1 **Subprocessors**. Google may engage Subprocessors to provide parts of the Services.

11.2 **Processing Restrictions**. Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that they are bound by written obligations: (i) that require them to provide at least the level of data protection required by the Safe Harbor Privacy Principles; and (ii) if Customer (or an authorized Customer Affiliate established in the European Economic Area) has entered into Model Contract Clauses with Google Inc., that impose the level of data protection required by the Model Contract Clauses.

11.3 **Customer Consent to Subprocessing**. Customer consents to Google subcontracting the processing of Customer Data to Subprocessors in accordance with the terms of the Agreement. If Customer (or an authorized Customer Affiliate established in the European Economic Area) enters into Model Contract Clauses with Google Inc., Customer consents to Google Inc. subcontracting the processing of Customer Data in accordance with the terms of the Model Contract Clauses.

11.4 **Additional information**. At the written request of the Customer, Google will provide additional information regarding Third Party Suppliers and their locations. Customer will send such requests to the Data Privacy Officer for Google Apps at: enterprise-dpo@google.com.

12. **Third Party Beneficiary**.

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 6.7 and Section 11.3 of this Data Processing Amendment.

13. **Effect of Amendment**.

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

Appendix 1: Categories of Data and Data Subjects

Categories of Data

Personal data submitted, stored, sent or received by Customer or End Users via the Services may include user IDs, email, documents, presentations, images, calendar entries, tasks and other electronic data.

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern End Users including employees, contractors and the personnel of customers, suppliers and subcontractors. Data subjects may also include individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

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

1. **Data Center & Network Security**.

(a) **Data Centers**.

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

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use 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 & 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:

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

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

3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS) available.

2. **Access and Site Controls**.

(a) **Site Controls**.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

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

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

(b) **Access Control**.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and for responding to security incidents.

Access Control and Privilege Management. Customer's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

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 aims to design 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; a need to know basis; and must be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include 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 & Authentication**.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per end user basis at the application layer. Google logically separates Customer's data, including data from different end users, from each other, and data for an authenticated end user will not be displayed to another end user (unless the former end user or administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

The 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 end users for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use.

(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 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. **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 always to the requirements set out in Section 11.2 of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Google Apps Data Processing Amendment, Version 1.3