Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.2)

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 one or more G Suite Agreement(s) (as defined below) and/or Complementary Product Agreements(s) (as defined below) (each, as amended from time to time, an "**Agreement**").

1. **Commencement**.

This Data Processing Amendment to G Suite and/or Complementary Product Agreement including its appendices (the "**Data Processing Amendment**") will be effective and replace any previously applicable data processing and security terms as from the Amendment Effective Date (as defined below).

This Data Processing Amendment supplements the applicable Agreement. Where that Agreement was entered into offline with Google Ireland Limited, this Data Processing Amendment supersedes the "Privacy" Clause in the Agreement (if applicable).

2. **Definitions**

2.1 Capitalized terms defined in the applicable Agreement apply to this Data Processing Amendment. In addition, in this Data Processing Amendment:

"**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

"**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, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.

"**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any of its Affiliates 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 any Google Sites functionality within the Services).

"**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

"**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the applicable Agreement.

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

"**Amendment Effective Date**" means the date on which Customer accepted, or the parties otherwise agreed to, this Data Processing Amendment.

"**Audited Services**" means:

a. those G Suite Core Services indicated as being in-scope for the relevant certification or report at https://cloud.google.com/security/compliance/services-in-scope/, provided that Google may only remove a G Suite Core Service from such URL by discontinuing that Service in accordance with the applicable Agreement; and

b. all other Services, unless the G Suite Services Summary or Complementary Product Services Summary indicates otherwise or the parties expressly agree otherwise in writing.

"**Complementary Product Agreement**" means: a Cloud Identity Agreement or other agreement under which Google agrees to provide identity services as such to Customer; Hire Agreement; or other agreement that incorporates this Data Processing Amendment by reference or states that it will apply if accepted by Customer.

"**Complementary Product Services Summary**" means the then-current description of the services provided under a Complementary Product Agreement, as set out in the applicable Agreement.

"**Customer Data**" means data submitted, stored, sent or received via the Services by Customer or End Users.

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

"**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.

"**Full Activation Date**" means: (a) if this Data Processing Amendment is automatically incorporated into the applicable Agreement, the Amendment Effective Date; or (b) if Customer accepted or the parties otherwise agreed to this Data Processing Amendment, the eighth day after the Amendment Effective Date.

"**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 or National 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.

"**G Suite Agreement**" means a G Suite Agreement; a G Suite for Education Agreement; a Google Cloud Master Agreement with G Suite Services Schedule; or any other agreement under which Google agrees to provide any services described in the G Suite Services Summary to Customer.

"**G Suite Services Summary**" means the then-current description of the G Suite services (including related editions), as set out at https://gsuite.google.com/terms/user_features.html (as may be updated by Google from time to time in accordance with the G Suite Agreement).

"**Model Contract Clauses**" or "MCCs" mean the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the EU GDPR.

"**Non-European Data Protection Law**" means data protection or privacy laws in force outside the EEA, Switzerland and the UK.

"**Notification Email Address**" means the email address(es) designated by Customer in the Admin Console, or in the Order Form or Ordering Document (as applicable), to receive certain notifications from Google. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.

"**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).

"**Service Specific Terms**" has the meaning given in the G Suite Agreement or Complementary Product Agreement, as applicable, or, if Customer's G Suite Agreement does not define "Service Specific Terms", means the then-current terms specific to one or more Core Services for G Suite set out at https://gsuite.google.com/terms/service-terms/.

"**Services**" means the following services, as applicable:

a. the Core Services for G Suite, as described in the G Suite Services Summary;

b. the Other Services for G Suite, as described in the G Suite Services Summary; and/or

c. the services described in the Complementary Product Services Summary.

"**Subprocessor**" means a third party authorized as another processor under this Data Processing Amendment 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.

"**Term**" means the period from the Amendment Effective Date until the end of Google's provision of the Services under the applicable Agreement, 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.

"**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 this Data Processing Amendment have the meanings given in the GDPR, irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

3. **Duration**. This Data Processing Amendment will, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by Google as described in this Data Processing Amendment.

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 behaviour 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 Data Processing Amendment. Except to the extent this Data Processing Amendment states otherwise, the terms of this Data Processing Amendment 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. Authorization by Third Party Controller. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants that its instructions and actions with respect to that Customer Personal Data, including its appointment of Google as another processor, have been authorized by the relevant controller.

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 and End Users' use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the applicable Agreement, including this Data Processing Amendment; and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment.

5.2.2 Google's Compliance with Instructions. As from the Full Activation Date (at the latest), Google will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless European or National Law to which Google is subject requires other processing of Customer Personal Data by Google, in which case Google will notify Customer (unless that law prohibits Google from doing so on important grounds of public interest) before such other processing. For clarity, Google will not process Customer Personal Data for Advertising purposes or serve Advertising in the Services.

5.3. **Additional Products**. If Google at its option makes any Additional Products available to Customer in accordance with the Additional Product Terms, and if Customer opts to install or use those Additional Products, the Services may allow those Additional Products to access Customer Personal Data as required for the interoperation of the Additional Products with the Services. For clarity, this Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products. Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services.

6. **Data Deletion**

6.1 **Deletion During Term**. Google will enable Customer and End Users to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to delete any Customer Data during the applicable Term and that Customer Data cannot be recovered by Customer or an End User (such as from the "trash"), 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 or National Law requires storage.

6.2 **Deletion on Term Expiry**. Subject to Section 6.3 (Deferred Deletion Instruction), on expiry of the applicable 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 or National Law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer is responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain.

6.3 **Deferred Deletion Instruction**. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Deletion on Term Expiry) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Data Processing Amendment will continue to apply to such Customer Data until its deletion by Google.

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 Security Compliance by Google Staff. Google will: (a) 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 (b) 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 applicable Agreement including this Data Processing Amendment; 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 or, at Google's discretion, by direct communication (for example, by phone call or an in-person meeting).

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 applicable 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. retaining copies of 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 **Compliance Certifications and SOC Reports**. Google will maintain at least the following for the Audited Services in order to evaluate the continued effectiveness of the Security Measures:

a. certificates for ISO 27001, ISO 27017 and ISO 27018, and

b. SOC 2 and SOC 3 reports produced by Google's Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the "**SOC Reports**"). 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 Reports available for review by Customer to demonstrate compliance by Google with its obligations under this Data Processing Amendment.

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 this Data Processing Amendment 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 (Compliance Certifications and SOC Reports) and this Section 7.5 (Reviews and Audits of Compliance).

b. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), Google will, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses 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 this Data Processing Amendment 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 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 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.

7.5.4 No Modification of MCCs. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Google LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data).

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 applicable Agreement including this Data Processing Amendment; 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 applicable 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 During Term), and to export Customer Data.

9.2 **Data Subject Requests**.

9.2.1 Customer's Responsibility for Requests. During the applicable 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 advise the data subject to submit their request to 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 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 (Customer's 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**. Google may store and process Customer Data anywhere Google or its Subprocessors maintain facilities, subject to Google's obligations under:

a. Section 10.2 (Transfers of Data) with respect to Model Contract Clauses or an Alternative Transfer Solution; and

b. the applicable Service Specific Terms (if any) with respect to data location.

10.2 **Transfers of Data**.

10.2.1 Google's Transfer Obligations. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data out of the EEA, Switzerland or the UK, and European Data Protection Law applies to the transfers of such data ("**Transferred Personal Data**") under any Agreement, Google will, in relation to Transferred Personal Data under all Agreements:

a. ensure that Google LLC enters into Model Contract Clauses with Customer as the exporter of such data if requested to do so by Customer, and ensure that the transfers are made in accordance with such Model Contract Clauses; and/or

b. offer an Alternative Transfer Solution in respect of such data, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

10.2.2 Customer's Transfer Obligations. In respect of Transferred Personal Data under any Agreement, Customer will:

a. enter into Model Contract Clauses as the exporter of such data, if under European Data Protection Law Google reasonably requires Customer to do so; and

b. use an Alternative Transfer Solution offered by Google in respect of such data and take any action (which may include execution of documents) strictly required to give full effect to such solution if under European Data Protection Law Google reasonably requires Customer to do so.

10.3 **Data Center Information**. Information about the locations of Google data centers is available at: https://www.google.com/about/datacenters/inside/locations/index.html (as may be updated by Google from time to time).

10.4 **Disclosure of Confidential Information Containing Personal Data**. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), Google will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer'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. **Subprocessors**

11.1 **Consent to Subprocessor Engagement**. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Amendment 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 Third Party Subprocessors**"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), the above authorizations constitute Customer's prior written consent to the subcontracting by Google LLC of the processing of Customer Data.

11.2 **Information about Subprocessors**. Information about Subprocessors, including their functions and locations, is available at https://gsuite.google.com/intl/en/terms/subprocessors.html (as may be updated by Google from time to time in accordance with this Data Processing Amendment).

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 this Data Processing Amendment) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Google as described in Section 10.2 (Transfers of Data); and

ii. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations described in Article 28(3) of the GDPR, as described in this Data Processing Amendment, 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 Third Party Subprocessor is engaged during the applicable Term, Google will, at least 30 days before the New Third Party 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 Third Party Subprocessor, object by terminating the applicable Agreement immediately upon written notice to Google. This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.

12. **Cloud Data Protection Team; Processing Records**

12.1 **Google's Cloud Data Protection Team**. Google's Cloud Data Protection Team can be contacted by Customer's Administrators at https://support.google.com/a/contact/googlecloud_dpr (while Administrators are signed in to their Admin Account) and/or by Customer by providing a notice to Google as described in the applicable Agreement.

12.2. **Google's Processing Records**. To the extent the GDPR requires Google to collect and maintain records of certain information relating to Customer, Customer will, where requested, use the Admin Console to 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.

13. **Liability**

13.1 **Liability Cap**. If Model Contract Clauses have been entered into as described in Section 10.2 (Transfers of Data) then, subject to Section 13.2 (Liability Cap Exclusions), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the applicable Agreement and such Model Contract Clauses combined will be limited to the Agreed Liability Cap for the relevant party.

13.2 **Liability Cap Exclusions**. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. **Third Party Beneficiary**

Notwithstanding anything to the contrary in the applicable Agreement, where Google LLC is not a party to such Agreement, Google LLC will be a third party beneficiary of Sections 7.5 (Reviews and Audits of Compliance), 11.1 (Consent to Subprocessor Engagement) and 13 (Liability).

15 **Effect of Amendment**

Notwithstanding anything to the contrary in the applicable Agreement, to the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the applicable Agreement, this Data Processing Amendment will govern. For clarity, if Customer has entered more than one Agreement, this Data Processing Amendment will amend each of the Agreements separately.

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 applicable Term plus the period from the expiry of such Term until deletion of all Customer Data by Google in accordance with the Data Processing Amendment.

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 Data Processing Amendment.

Categories of Data

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

Appendix 2: Security Measures

As from the Amendment 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. 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 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 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. 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.

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. Subject to any Customer instructions to the contrary (for example, in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data, and logically separates each End User's data from the data of other End Users, and data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared).

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 use 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 this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.