Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.3)

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 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 and set out at https://gsuite.google.com/terms/mcc_terms.html.
- "**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 the 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:
        - a. Section 10.2 (Transfers of Data) with respect to the Model Contract Clauses or Alternative Transfer Solution; and
        - b. the applicable Service Specific Terms (if any) with respect to data location.
    - 10.2 **Transfers of Data**. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data from the EEA, Switzerland or the UK to any third country that does not ensure an adequate level of protection under European Data Protection Law, and

European Data Protection Law applies to those transfers, then:

- a. if Customer (as data exporter) enters into the Model Contract Clauses with Google LLC (as data importer) within the Admin Console, then:
    - i. the transfers will be subject to the Model Contract Clauses; and
    - ii. Google will ensure that Google LLC complies with its obligations under the Model Contract Clauses in respect of those transfers; or
- b. if Customer does not enter into the Model Contract Clauses as described in Section 10.2(a), then:
    - i. if an Alternative Transfer Solution is made available by Google: (A) Customer will be deemed to be using it and will take any action (which may include execution of documents) strictly required to give it full effect; and (B) Google will ensure that the transfers are made in accordance with such Alternative Transfer Solution; or
    - ii. if an Alternative Transfer Solution is not made available by Google: (A) Customer (as data exporter) will be deemed to have entered into the Model Contract Clauses with Google LLC (as data importer); (B) the transfers will be subject to the Model Contract Clauses; and (C) Google will ensure Google LLC complies with its obligations under the Model Contract Clauses in respect of those transfers; and
- c. if Customer has entered into the Model Contract Clauses but reasonably determines subsequently that they do not provide an adequate level of protection, then:
    - i. if an Alternative Transfer Solution is made available by Google, Customer may, by notifying Google LLC via Google's Cloud Data Protection

Team in accordance with Section 12.1 (Google's Cloud Data Protection Team), terminate any Model Contract Clauses applicable under Section 10.2(a), such that Section 10.2(b)(i) will apply; or

- ii. if an Alternative Transfer Solution is not made available by Google, Customer may terminate the Agreement immediately by notifying Google.

- 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 the Model Contract Clauses or Alternative Transfer Solution, as applicable under 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 by notifying 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 (w hile 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 the 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), 10.2 (Data Transfers), 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.

CONTRATO DE ENCARGO DE TRATAMIENTO (Versión traducida no oficial)

Enmienda de procesamiento de datos a G Suite y / o Acuerdo de producto complementario (Versión 2.3)

El cliente que acepta estos términos ("Cliente") y Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., o cualquier otra entidad que controle directa o indirectamente, esté controlada por, o esté bajo control común con Google LLC (según corresponda, "Google"), haya celebrado uno o más acuerdos de G Suite (como se define a continuación) y / o Acuerdos de productos complementarios (como se definen a continuación) (cada uno, con las enmiendas periódicas, un "Acuerdo").

1. Comienzo.
Esta Enmienda de procesamiento de datos de G Suite y / o Acuerdo de producto complementario, incluidos sus apéndices (la "Enmienda de procesamiento de datos") entrará en vigencia y reemplazará cualquier procesamiento de datos y términos de seguridad previamente aplicables a partir de la Fecha de vigencia de la Enmienda (como se define a continuación).
Esta Enmienda de procesamiento de datos complementa el Acuerdo aplicable. Cuando ese Acuerdo se celebró fuera de línea con Google Ireland Limited, esta Enmienda de procesamiento de datos reemplaza la Cláusula de "Privacidad" en el Acuerdo (si corresponde).
2. Definiciones
2.1 Los términos en mayúscula definidos en el Acuerdo aplicable se aplican a esta Enmienda de procesamiento de datos. Además, en esta Enmienda de procesamiento de datos:
“Productos adicionales” hace referencia a productos, servicios y aplicaciones que no forman parte de los Servicios pero que pueden ser accesibles, a través de la Consola de administración o de otro modo, para su uso con los Servicios.
"Controles de seguridad adicionales" significa recursos de seguridad, características, funcionalidad y / o controles que el Cliente puede usar a su opción y / o según lo determine, incluida la Consola de administración, encriptación, registro y monitoreo, administración de identidad y acceso, escaneo de seguridad y cortafuegos.
"Publicidad" se refiere a los anuncios en línea que Google muestra a los Usuarios finales, excluyendo cualquier anuncio que el Cliente elija expresamente que Google o cualquiera de sus Afiliados se muestre en relación con los Servicios en virtud de un acuerdo separado (por ejemplo, anuncios de Google AdSense implementados por el Cliente en un sitio web creado por el Cliente utilizando cualquier funcionalidad de Google Sites dentro de los Servicios).
"Afiliado" significa cualquier entidad que controle, controle o esté bajo control común con una parte, donde "control" se define como: (a) la propiedad de al menos el cincuenta por ciento (50%) del capital social o de los intereses beneficiarios de la entidad; (b) el derecho a votar o nombrar a la mayoría del consejo de administración u otro órgano de gobierno de la entidad; o (c) el poder de ejercer una influencia controladora sobre la administración o las políticas de la entidad.
"Límite de responsabilidad acordado" significa el monto máximo monetario o basado en pagos al que se limita la responsabilidad de una parte en virtud del Acuerdo aplicable.
“Solución de transferencia alternativa” significa una solución, distinta de las Cláusulas contractuales modelo, que permite la transferencia legal de datos personales a un tercer país de acuerdo con la Ley europea de protección de datos.
"Fecha de vigencia de la enmienda" significa la fecha en la que el Cliente aceptó, o las partes acordaron de otro modo, esta Enmienda de procesamiento de datos.
"Servicios auditados" significa:

una. aquellos servicios centrales de G Suite indicados como incluidos en el alcance de la certificación o informe correspondiente en https://cloud.google.com/security/compliance/services-in-scope/, siempre que Google solo pueda eliminar un servicio central de G Suite de dicha URL interrumpiendo ese Servicio de acuerdo con el Acuerdo aplicable; y
B. todos los demás Servicios, a menos que el Resumen de Servicios de G Suite o el Resumen de Servicios de Productos Complementarios indiquen lo contrario o las partes acuerden expresamente lo contrario por escrito.
"Acuerdo de producto complementario" significa: un Acuerdo de identidad de Cloud u otro acuerdo en virtud del cual Google acepta proporcionar servicios de identidad como tales al Cliente; Acuerdo de alquiler; u otro acuerdo que incorpore esta Enmienda de procesamiento de datos por referencia o establezca que se aplicará si el Cliente lo acepta.
“Resumen de servicios de productos complementarios” significa la descripción vigente en ese momento de los servicios prestados en virtud de un Acuerdo de producto complementario, según se establece en el Acuerdo aplicable.
"Datos del cliente" se refiere a los datos enviados, almacenados, enviados o recibidos a través de los Servicios por el Cliente o los Usuarios finales.
"Datos personales del cliente" se refiere a los datos personales contenidos en los Datos del cliente.
"Incidente de datos" hace referencia a una violación de la seguridad de Google que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a los Datos del cliente en sistemas administrados o controlados por Google de otra manera.
“EEE” significa el Espacio Económico Europeo.
“Fecha de activación completa” significa: (a) si esta Enmienda de procesamiento de datos se incorpora automáticamente al Acuerdo aplicable, la Fecha de vigencia de la Enmienda; o (b) si el Cliente aceptó o las partes acordaron de otro modo esta Enmienda de procesamiento de datos, el octavo día después de la Fecha de vigencia de la Enmienda.
"RGPD UE" hace referencia al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 sobre la protección de las personas físicas con respecto ad al tratamiento de datos personales y a la libre circulación de dichos datos, y por la que se deroga la Directiva 95/46 / CE.
“Ley europea de protección de datos” significa, según corresponda: (a) el RGPD; y / o (b) la Ley Federal de Protección de Datos de 19 de junio de 1992 (Suiza).
"Legislación europea o nacional" significa, según corresponda: (a) la legislación de la UE o de los Estados miembros de la UE (si el RGPD de la UE se aplica al procesamiento de datos personales del cliente); y / o (b) la legislación del Reino Unido o una parte de el Reino Unido (si el RGPD del Reino Unido se aplica al procesamiento de datos personales del cliente).
"RGPD" significa, según corresponda: (a) el RGPD de la UE; y / o (b) el RGPD del Reino Unido.
"Auditor externo de Google" hace referencia a un auditor externo calificado, independiente y designado por Google, cuya identidad actual en ese momento Google revelará al Cliente.
"Acuerdo de G Suite" hace referencia a un Acuerdo de G Suite; un Acuerdo de G Suite para Centros Educativos; un acuerdo maestro de Google Cloud con el programa de servicios de G Suite; o cualquier otro acuerdo en virtud del cual Google acepta proporcionar al Cliente los servicios descritos en el Resumen de servicios de G Suite.
"Resumen de servicios de G Suite" hace referencia a la descripción vigente en ese momento de los servicios de G Suite (incluidas las ediciones relacionadas), según se establece en https://gsuite.google.com/terms/user_features.html (según puede ser actualizado por Google desde de vez en cuando de acuerdo con el Acuerdo de G Suite).
"Cláusulas contractuales modelo" o "MCC" se refieren a cláusulas estándar de protección de datos para la transferencia de datos personales a procesadores establecidos en terceros países que no garantizan un nivel adecuado de protección de datos, como se describe en el artículo 46 del RGPD de la UE y se establece en https://gsuite.google.com/terms/mcc_terms.html.

“Ley de protección de datos no europea” hace referencia a las leyes de privacidad o protección de datos vigentes fuera del EEE, Suiza y el Reino Unido.
"Dirección de correo electrónico de notificación" hace referencia a las direcciones de correo electrónico designadas por el Cliente en la Consola de administración, o en el Formulario de pedido o Documento de pedido (según corresponda), para recibir determinadas notificaciones de Google. El cliente es responsable de utilizar la Consola de administración para asegurarse de que su dirección de correo electrónico de notificación se mantenga actualizada y válida.
“Documentación de seguridad” hace referencia a todos los documentos e información que Google pone a disposición en la Sección 7.5.1 (Revisiones de la documentación de seguridad).
"Medidas de seguridad" tiene el significado que se le da en la Sección 7.1.1 (Medidas de seguridad de Google).
"Términos específicos del servicio" tiene el significado que se le da en el Acuerdo de G Suite o en el Acuerdo de producto complementario, según corresponda, o, si el Acuerdo de G Suite del cliente no define "Términos específicos del servicio", se refiere a los términos vigentes en ese momento específicos de uno o más de los principales Los servicios para G Suite se establecen en https://gsuite.google.com/terms/service-terms/.
"Servicios" significa los siguientes servicios, según corresponda:
A. los Servicios Principales para G Suite, como se describe en el Resumen de Servicios de G Suite;
B. los Otros servicios para G Suite, como se describe en el Resumen de servicios de G Suite; y / o
C. los servicios descritos en el Resumen de servicios de productos complementarios.
“Subprocesador” significa un tercero autorizado como otro procesador en virtud de esta Enmienda de procesamiento de datos para tener acceso lógico y procesar los Datos del cliente con el fin de proporcionar partes de los Servicios y TSS.
"Autoridad supervisora" significa, según corresponda: (a) una "autoridad supervisora" según se define en el RGPD de la UE; y / o (b) el "Comisionado" según se define en el RGPD del Reino Unido.
"Plazo" significa el período desde la Fecha de entrada en vigencia de la Enmienda hasta el final de la prestación de los Servicios por parte de Google en virtud del Acuerdo aplicable, incluido, si corresponde, cualquier período durante el cual la prestación de los Servicios pueda suspenderse y cualquier período posterior a la rescisión durante el cual Google puede continuar brindando los Servicios con fines de transición.
"RGPD del Reino Unido" hace referencia al RGPD de la UE en su forma enmendada e incorporada a la ley del Reino Unido en virtud de la Ley de (Retirada) de la Unión Europea del Reino Unido de 2018, si está en vigor.
2.2. Los términos "datos personales", "sujeto de datos", "procesamiento", "controlador" y "procesador", tal como se utilizan en esta Enmienda de procesamiento de datos, tienen los significados dados en el RGPD, independientemente de si la ley europea de protección de datos o los datos no europeos Se aplica la Ley de Protección.
3. Duración. Esta Enmienda de procesamiento de datos, a pesar de la expiración del Plazo, permanecerá en vigencia hasta que Google elimine todos los Datos del cliente, y expirará automáticamente, como se describe en esta Enmienda de procesamiento de datos.
4. Alcance de la Ley de Protección de Datos.
4.1 Aplicación de la legislación europea. Las partes reconocen que la Ley Europea de Protección de Datos se aplicará al procesamiento de los Datos Personales del Cliente si, por ejemplo:
A. el procesamiento se lleva a cabo en el contexto de las actividades de un establecimiento del Cliente en el territorio del EEE o el Reino Unido; y / o
B. los Datos personales del cliente son datos personales relacionados con sujetos de datos que se encuentran en el EEE o el Reino Unido y el procesamiento se relaciona con la oferta de bienes o servicios en el EEE o el Reino Unido, o el seguimiento de su comportamiento en el EEE o el REINO UNIDO.

4.2 Aplicación de la legislación extraeuropea. Las partes reconocen que la ley de protección de datos no europea también puede aplicarse a los procesamientos de datos personales del cliente.
4.3 Aplicación de la Enmienda de Procesamiento de Datos. Excepto en la medida en que esta Enmienda de procesamiento de datos establezca lo contrario, los términos de esta Enmienda de procesamiento de datos se aplicarán independientemente de si la Ley europea de protección de datos o la Ley de protección de datos no europea se aplica al procesamiento de los Datos personales del cliente.
5. Tratamiento de datos.
5.1 Funciones y cumplimiento normativo; Autorización.
5.1.1. Responsabilidades del procesador y del controlador. Si la ley europea de protección de datos se aplica al procesamiento de datos personales del cliente:
A. el tema y los detalles del procesamiento se describen en el Apéndice 1;
B. Google es un procesador de los Datos personales del cliente según la Ley europea de protección de datos;
C. El Cliente es un controlador o procesador, según corresponda, de los Datos personales del Cliente según la Ley europea de protección de datos; y
D. cada parte cumplirá con las obligaciones que le son aplicables en virtud de la Ley europea de protección de datos con respecto al procesamiento de los Datos personales del cliente.
5.1.2. Autorización por parte del controlador externo. Si la Ley europea de protección de datos se aplica al procesamiento de los Datos personales del cliente y el Cliente es un procesador, el Cliente garantiza que sus instrucciones y acciones con respecto a esos Datos personales del cliente, incluido su nombramiento de Google como otro procesador, han sido autorizados por el controlador correspondiente. .
5.1.3. Responsabilidades bajo la ley no europea. Si la Ley de protección de datos no europea se aplica al procesamiento de los Datos personales del cliente por cualquiera de las partes, la parte correspondiente cumplirá con las obligaciones que le sean aplicables en virtud de esa ley con respecto al procesamiento de esos Datos personales del cliente.
5.2 Alcance del procesamiento.
5.2.1 Instrucciones del cliente. El Cliente indica a Google que procese los Datos personales del Cliente solo de acuerdo con la ley aplicable: (a) para proporcionar los Servicios y TSS; (b) según se especifique más a través del uso de los Servicios por parte del Cliente y los Usuarios finales (incluida la Consola de administración y otras funciones de los Servicios) y TSS; (c) según se documente en la forma del Acuerdo aplicable, incluida esta Enmienda de procesamiento de datos; y (d) según se documente con más detalle en cualquier otra instrucción escrita proporcionada por el Cliente y reconocida por Google como instrucciones para los fines de esta Enmienda de procesamiento de datos.
5.2.2 Cumplimiento de las instrucciones por parte de Google. A partir de la Fecha de activación completa (a más tardar), Google cumplirá con las instrucciones descritas en la Sección 5.2.1 (Instrucciones del cliente) (incluso con respecto a las transferencias de datos) a menos que la legislación europea o nacional a la que esté sujeto Google requiera otro procesamiento de Datos personales del cliente de Google, en cuyo caso Google notificará al Cliente (a menos que la ley prohíba a Google hacerlo por motivos importantes de interés público) antes de dicho otro procesamiento. Para mayor claridad, Google no procesará los Datos personales del cliente con fines publicitarios ni ofrecerá publicidad en los Servicios.
5.3. Productos adicionales. Si Google, a su criterio, pone a disposición del Cliente productos adicionales de acuerdo con las Condiciones de productos adicionales, y si el Cliente opta por instalar o utilizar esos Productos adicionales, los Servicios pueden permitir que esos Productos adicionales accedan a los Datos personales del Cliente según sea necesario para la interoperación de los Productos Adicionales con los Servicios. Para mayor claridad, esta Enmienda de procesamiento de datos no se aplica al procesamiento de datos personales en relación con la provisión de Productos

adicionales instalados o utilizados por el Cliente, incluidos los datos personales transmitidos hacia o desde dichos Productos adicionales. El Cliente puede utilizar la funcionalidad de los Servicios para habilitar o deshabilitar Productos Adicionales y no está obligado a utilizar Productos Adicionales para utilizar los Servicios.

6. Eliminación de datos

6.1 Eliminación durante el período. Google permitirá que el Cliente y los Usuarios finales eliminen los Datos del cliente durante el Período de vigencia correspondiente de manera coherente con la funcionalidad de los Servicios. Si el Cliente o un Usuario final utiliza los Servicios para eliminar los Datos del cliente durante el Plazo aplicable y el Cliente o un Usuario final no pueden recuperar los Datos del cliente (por ejemplo, de la "papelera"), este uso constituirá una instrucción para Google para eliminar los Datos del cliente relevantes de los sistemas de Google de acuerdo con la ley aplicable. Google cumplirá con esta instrucción tan pronto como sea razonablemente posible y dentro de un período máximo de 180 días, a menos que la legislación europea o nacional exija su almacenamiento.

6.2 Eliminación al expirar el plazo. Sujeto a la Sección 6.3 (Instrucción de Eliminación Diferida), al expirar el Plazo aplicable, el Cliente indica a Google que elimine todos los Datos del Cliente (incluidas las copias existentes) de los sistemas de Google de acuerdo con la ley aplicable. Google cumplirá con esta instrucción tan pronto como sea razonablemente posible y dentro de un período máximo de 180 días, a menos que la legislación europea o nacional requiera almacenamiento. Sin perjuicio de la Sección 9.1 (Acceso; Rectificación; Procesamiento restringido; Portabilidad), el Cliente es responsable de exportar, antes de que expire el Plazo aplicable, cualquier Dato del Cliente que desee retener.

6.3 Instrucción de eliminación diferida. En la medida en que también se procesen los Datos del Cliente cubiertos por la instrucción de eliminación descrita en la Sección 6.2 (Eliminación por Vencimiento del Término), cuando el Término aplicable bajo la Sección 6.2 expire, en relación con un Acuerdo con un Término continuo, dicha instrucción de eliminación solo tomará efecto con respecto a dichos Datos del Cliente cuando expire el Período de vigencia. Para mayor claridad, esta Enmienda de procesamiento de datos seguirá aplicándose a dichos Datos del cliente hasta que Google la elimine.

7. Seguridad de los datos.

7.1 Medidas de seguridad, controles y asistencia de Google.

7.1.1 Medidas de seguridad de Google. Google implementará y mantendrá medidas técnicas y organizativas para proteger los Datos del Cliente contra la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal, como se describe en el Apéndice 2 (las "Medidas de seguridad"). Las Medidas de Seguridad incluyen medidas para encriptar datos personales; para ayudar a garantizar la confidencialidad, integridad, disponibilidad y resistencia continuas de los sistemas y servicios de Google; para ayudar a restaurar el acceso oportuno a los datos personales después de un incidente; y para pruebas periódicas de eficacia. Google puede actualizar las Medidas de seguridad de vez en cuando, siempre que dichas actualizaciones no den como resultado la degradación de la seguridad general de los Servicios.

7.1.2 Cumplimiento de seguridad por parte del personal de Google. Google: (a) tomará las medidas adecuadas para garantizar el cumplimiento de las Medidas de seguridad por parte de sus empleados, contratistas y subprocesadores en la medida que sea aplicable a su alcance de desempeño, y (b) se asegurará de que todas las personas autorizadas para procesar los Datos personales del cliente estén bajo una obligación de confidencialidad.

7.1.3 Controles de seguridad adicionales. Google pondrá a disposición Controles de seguridad adicionales para: (a) permitir que el Cliente tome medidas para proteger los Datos del Cliente; y (b) proporcionar al Cliente información sobre cómo proteger, acceder y utilizar los Datos del Cliente.

7.1.4 Asistencia de seguridad de Google. Google (teniendo en cuenta la naturaleza del procesamiento de los Datos personales del cliente y la información disponible para Google) ayudará

al Cliente a garantizar el cumplimiento de sus obligaciones de conformidad con los artículos 32 a 34 del RGPD mediante:
A. implementar y mantener las Medidas de seguridad de acuerdo con la Sección 7.1.1 (Medidas de seguridad de Google);
B. poner Controles de seguridad adicionales a disposición del Cliente de acuerdo con la Sección 7.1.3 (Controles de seguridad adicionales);
C. cumplir con los términos de la Sección 7.2 (Incidentes de datos);
D. proporcionar al Cliente la Documentación de seguridad de acuerdo con la Sección 7.5.1 (Revisiones de la Documentación de seguridad) y la información contenida en el Acuerdo aplicable, incluida esta Enmienda de procesamiento de datos; y
mi. si las subsecciones (a) - (d) anteriores son insuficientes para que el Cliente cumpla con dichas obligaciones, a solicitud del Cliente, brindando asistencia adicional razonable.
7.2 Incidentes de datos
7.2.1 Notificación de incidentes. Google notificará al Cliente de inmediato y sin demoras indebidas después de tener conocimiento de un Incidente de datos y tomará las medidas razonables para minimizar el daño y proteger los Datos del cliente.
7.2.2 Detalles del incidente de datos. La notificación de Google de un Incidente de datos describirá, en la medida de lo posible, la naturaleza del Incidente de datos, las medidas tomadas para mitigar los riesgos potenciales y las medidas que Google recomienda que el Cliente tome para abordar el Incidente de datos.
7.2.3 Entrega de notificación. Las notificaciones de cualquier incidente de datos se enviarán a la dirección de correo electrónico de notificación o, a discreción de Google, mediante comunicación directa (por ejemplo, por llamada telefónica o una reunión en persona).
7.2.4 No evaluación de los datos del cliente por parte de Google. Google no tiene la obligación de evaluar los Datos del cliente para identificar la información sujeta a requisitos legales específicos.
7.2.5 Sin reconocimiento de fallas por parte de Google. La notificación o respuesta de Google a un Incidente de datos en virtud de esta Sección 7.2 (Incidentes de datos) no se interpretará como un reconocimiento por parte de Google de cualquier falla o responsabilidad con respecto al Incidente de datos.
7.3. Responsabilidades y evaluación de seguridad del cliente.
7.3.1 Responsabilidades de seguridad del cliente. Sin perjuicio de las obligaciones de Google en virtud de las Secciones 7.1 (Medidas de seguridad, controles y asistencia de Google) y 7.2 (Incidentes de datos), y en cualquier otra parte del Acuerdo aplicable, el Cliente es responsable de su uso de los Servicios y su almacenamiento de cualquier copia de los Datos del cliente fuera de Los sistemas de Google o de los subprocesadores de Google, incluidos:
A. utilizar los Servicios y los Controles de seguridad adicionales para garantizar un nivel de seguridad adecuado al riesgo con respecto a los Datos del cliente;
B. asegurar las credenciales de autenticación de la cuenta, los sistemas y los dispositivos que utiliza el Cliente para acceder a los Servicios; y
C. conservar copias de sus Datos de cliente según corresponda.
7.3.2 Evaluación de seguridad del cliente. El cliente acepta, en base a su actual intención de uso determinado de los Servicios, que los Servicios, las Medidas de seguridad, los Controles de seguridad adicionales y los compromisos de Google en virtud de esta Sección 7 (Seguridad de datos): (a) satisfagan las necesidades del Cliente, incluso con respecto a cualquier obligación de seguridad del Cliente en virtud de la Ley europea de protección de datos y / o la Ley de protección de datos no europea, según corresponda, y (b) proporcionar un nivel de seguridad adecuado al riesgo con respecto a los Datos del cliente.
7.4 Certificaciones de cumplimiento e informes SOC. Google mantendrá al menos lo siguiente para los Servicios auditados con el fin de evaluar la efectividad continua de las Medidas de seguridad:
A. certificados para ISO 27001, ISO 27017 e ISO 27018, y

B. Informes SOC 2 y SOC 3 elaborados por el auditor externo de Google y actualizados anualmente en función de una auditoría realizada al menos una vez cada 12 meses (los "Informes SOC"). Google puede agregar estándares en cualquier momento. Google puede reemplazar un Informe SOC con una alternativa equivalente o mejorada.

7.5 Revisiones y auditorías de cumplimiento

7.5.1 Revisiones de la documentación de seguridad. Google pondrá los Informes SOC a disposición del Cliente para que los revise el Cliente a fin de demostrar el cumplimiento por parte de Google de sus obligaciones en virtud de esta Enmienda de procesamiento de datos.

7.5.2 Derechos de auditoría del cliente.

A. Si la Ley europea de protección de datos se aplica al procesamiento de los Datos personales del cliente, Google permitirá que el Cliente o un auditor independiente designado por el Cliente realice auditorías (incluidas inspecciones) para verificar el cumplimiento de Google con sus obligaciones en virtud de esta Enmienda de procesamiento de datos de acuerdo con la Sección 7.5. 3 (Condiciones comerciales adicionales para revisiones y auditorías). Google contribuirá a dichas auditorías como se describe en la Sección 7.4 (Certificaciones de cumplimiento e informes SOC) y esta Sección 7.5 (Revisiones y auditorías de cumplimiento).

B. Si el Cliente ha celebrado las Cláusulas del contrato modelo como se describe en la Sección 10.2 (Transferencias de datos), Google permitirá al Cliente o un auditor independiente designado por el Cliente realizar auditorías como se describe en las Cláusulas del contrato modelo de acuerdo con la Sección 7.5.3 (Términos comerciales adicionales para revisiones y auditorías).

C. El Cliente puede realizar una auditoría para verificar el cumplimiento de Google con sus obligaciones en virtud de esta Enmienda de procesamiento de datos mediante la revisión de la Documentación de seguridad (que refleja el resultado de las auditorías realizadas por el Auditor externo de Google).

7.5.3 Condiciones comerciales adicionales para revisiones y auditorías.

A. El Cliente debe enviar cualquier solicitud de revisión del informe SOC 2 según la Sección 7.5.1 o auditorías según la Sección 7.5.2 (a) o 7.5.2 (b) al Equipo de Protección de Datos en la Nube de Google como se describe en la Sección 12 (Equipo de Protección de Datos en la Nube ; Procesamiento de registros).

B. Tras la recepción por parte de Google de una solicitud en virtud de la Sección 7.5.3 (a), Google y el Cliente analizarán y acordarán por adelantado: (i) las fechas razonables y los controles de seguridad y confidencialidad aplicables a cualquier revisión del SOC 2 informe según la Sección 7.5.1; y (ii) la fecha razonable de inicio, alcance y duración de los controles de seguridad y confidencialidad aplicables a cualquier auditoría bajo la Sección 7.5.2 (a) o 7.5.2 (b).

C. Google puede cobrar una tarifa (basada en los costos razonables de Google) por cualquier auditoría según la Sección 7.5.2 (a) o 7.5.2 (b). Google proporcionará al Cliente más detalles de cualquier tarifa aplicable y la base de su cálculo, antes de dicha auditoría. El Cliente será responsable de los honorarios cobrados por cualquier auditor designado por el Cliente para ejecutar dicha auditoría.

D. Google puede oponerse por escrito a un auditor designado por el Cliente para realizar cualquier auditoría de conformidad con la Sección 7.5.2 (a) o 7.5.2 (b) si el auditor, en la opinión razonable de Google, no está adecuadamente calificado o no es independiente, un competidor de Google. , o de otra manera manifiestamente inadecuada. Cualquier objeción de este tipo por parte de Google requerirá que el Cliente nombre a otro auditor o realice la auditoría él mismo.

7.5.4 Sin modificación de MCC. Nada en esta Sección 7.5 (Revisiones y auditorías de cumplimiento) varía o modifica los derechos u obligaciones del Cliente o de Google LLC en virtud de las Cláusulas de contrato modelo celebradas como se describe en la Sección 10.2 (Transferencias de datos).

8. Evaluaciones de impacto y consultas. Google (teniendo en cuenta la naturaleza del procesamiento y la información disponible para Google) ayudará al Cliente a garantizar el cumplimiento de sus obligaciones de conformidad con los artículos 35 y 36 del GDPR, mediante:

A. proporcionar Controles de seguridad adicionales de acuerdo con la Sección 7.1.3 (Controles de seguridad adicionales) y la Documentación de seguridad de acuerdo con la Sección 7.5.1 (Revisiones de la documentación de seguridad);
B. proporcionar la información contenida en el Acuerdo aplicable, incluida esta Enmienda de procesamiento de datos; y
C. si las subsecciones (a) y (b) anteriores son insuficientes para que el Cliente cumpla con dichas obligaciones, a solicitud del Cliente, brindando asistencia adicional razonable.
9. Acceso, etc .; Derechos del interesado; Exportación de datos
9.1 Acceso; Rectificación; Procesamiento restringido; Portabilidad. Durante el Plazo aplicable, Google habilitará al Cliente, en un de manera coherente con la funcionalidad de los Servicios, para acceder, rectificar y restringir el procesamiento de los Datos del Cliente, incluso a través de la función de eliminación proporcionada por Google como se describe en la Sección 6.1 (Eliminación durante el Plazo), y para exportar los Datos del Cliente.
9.2 Solicitudes de sujetos de datos.
9.2.1 Responsabilidad del cliente por las solicitudes. Durante el Plazo aplicable, si el Equipo de Protección de Datos en la Nube de Google recibe una solicitud de un interesado en relación con los Datos Personales del Cliente, y la solicitud identifica al Cliente, Google le informará al interesado que envíe su solicitud al Cliente. El Cliente será responsable de responder a dicha solicitud, incluido, cuando sea necesario, mediante el uso de la funcionalidad de los Servicios.
9.2.2 Solicitud de asistencia del interesado de Google. Google (teniendo en cuenta la naturaleza del procesamiento de los Datos personales del cliente) ayudará al Cliente a cumplir con sus obligaciones en virtud del Capítulo III del RGPD para responder a las solicitudes de ejercicio de los derechos del interesado mediante:
A. proporcionar Controles de seguridad adicionales de acuerdo con la Sección 7.1.3 (Controles de seguridad adicionales);
B. cumplir con las Secciones 9.1 (Acceso; Rectificación; Procesamiento restringido; Portabilidad) y 9.2.1 (Responsabilidad del cliente por las solicitudes); y
C. si las subsecciones (a) y (b) anteriores son insuficientes para que el Cliente cumpla con dichas obligaciones, a solicitud del Cliente, brindando asistencia adicional razonable.
10. Transferencias de datos
10.1 Instalaciones de procesamiento y almacenamiento de datos. Google puede almacenar y procesar los Datos del Cliente en cualquier lugar donde Google o sus Subprocesadores mantengan instalaciones, sujeto a:
A. Sección 10.2 (Transferencias de datos) con respecto a las Cláusulas del contrato modelo o la Solución de transferencia alternativa; y
B. los Términos específicos del servicio aplicables (si los hubiera) con respecto a la ubicación de los datos.
10.2 Transferencias de datos. Si el almacenamiento y / o procesamiento de datos personales del cliente implica transferencias de datos personales del cliente desde el EEE, Suiza o el Reino Unido a cualquier tercer país que no garantice un nivel adecuado de protección según la ley europea de protección de datos, y se aplica la ley europea de protección de datos. a esas transferencias, entonces:
A. si el Cliente (como exportador de datos) entra en las Cláusulas de contrato modelo con Google LLC (como importador de datos) dentro de la Consola de administración, entonces:
I. las transferencias estarán sujetas a las Cláusulas de Contrato Modelo; y
ii. Google se asegurará de que Google LLC cumpla con sus obligaciones en virtud de las Cláusulas del contrato modelo con respecto a esas transferencias; o
B. si el Cliente no suscribe las Cláusulas del contrato modelo como se describe en la Sección 10.2 (a), entonces:

I. si Google pone a disposición una Solución de transferencia alternativa: (A) se considerará que el Cliente la está utilizando y tomará cualquier acción (que puede incluir la ejecución de documentos) estrictamente necesaria para que tenga pleno efecto; y (B) Google se asegurará de que las transferencias se realicen de acuerdo con dicha Solución de transferencia alternativa; o
ii. si Google no pone a disposición una Solución de transferencia alternativa: (A) Se considerará que el Cliente (como exportador de datos) ha suscrito las Cláusulas de contrato modelo con Google LLC (como importador de datos); (B) las transferencias estarán sujetas a las Cláusulas del Contrato Modelo; y (C) Google se asegurará de que Google LLC cumpla con sus obligaciones en virtud de las Cláusulas del contrato modelo con respecto a esas transferencias; y
C. Si el Cliente ha suscrito las Cláusulas del contrato modelo, pero posteriormente determina razonablemente que no brindan un nivel adecuado de protección, entonces:
I. si Google pone a disposición una Solución de transferencia alternativa, el Cliente puede, notificando a Google LLC a través del Equipo de protección de datos en la nube de Google de acuerdo con la Sección 12.1 (Equipo de protección de datos en la nube de Google), rescindir cualquier Cláusula de contrato modelo aplicable en virtud de la Sección 10.2 (a), de manera que se aplique la Sección 10.2 (b) (i); o
ii. Si Google no pone a disposición una Solución de transferencia alternativa, el Cliente puede rescindir el Acuerdo de inmediato notificando a Google.
10.3 Información del centro de datos. La información sobre las ubicaciones de los centros de datos de Google está disponible en:
https://www.google.com/about/datacenters/inside/locations/index.html
(según lo pueda actualizar Google de vez en cuando).
10.4 Divulgación de información confidencial que contenga datos personales. Si el Cliente ha celebrado Cláusulas de contrato modelo como se describe en la Sección 10.2 (Transferencias de datos), Google, sin perjuicio de cualquier término en contrario en el Acuerdo aplicable, se asegurará de que cualquier divulgación de la Información confidencial del Cliente que contenga datos personales y cualquier notificación relacionada con cualquier divulgación de este tipo se realizará de acuerdo con dichas Cláusulas de contrato modelo.
11. Subprocesadores
11.1 Consentimiento para la participación del subprocesador. El Cliente autoriza específicamente la contratación como Subencargados del tratamiento de: (a) aquellas entidades que figuran en la Fecha de entrada en vigor de la Enmienda en la URL especificada en la Sección 11.2 (Información sobre Subencargados del tratamiento); y (b) todos los demás afiliados de Google de vez en cuando. Además, sin perjuicio de Sección 11.4 (Oportunidad de oponerse a los cambios del subprocesador), el Cliente generalmente autoriza la contratación como Subprocesadores de cualquier otro tercero ("Nuevos subprocesadores de terceros"). Si el Cliente ha suscrito Cláusulas de contrato modelo como se describe en la Sección 10.2 (Transferencias de datos), las autorizaciones anteriores constituyen el consentimiento previo por escrito del Cliente a la subcontratación por parte de Google LLC del procesamiento de los Datos del cliente.
11.2 Información sobre subprocesadores. La información sobre los subprocesadores, incluidas sus funciones y ubicaciones, está disponible en https://gsuite.google.com/intl/en/terms/subprocessors.html (según pueda ser actualizado por Google de vez en cuando de acuerdo con esta Enmienda de procesamiento de datos).
11.3 Requisitos para la contratación del subprocesador. Al contratar cualquier subprocesador, Google:
A. garantizar mediante un contrato escrito que:
I. el Subprocesador solo accede y utiliza los Datos del Cliente en la medida necesaria para cumplir con las obligaciones subcontratadas, y lo hace de acuerdo con el Acuerdo (incluida esta Enmienda de procesamiento de datos) y las Cláusulas del contrato modelo o Solución de transferencia alternativa, según corresponda en la Sección 10.2 (Transferencias de datos); y

ii. si el RGPD se aplica al procesamiento de Datos personales del cliente, las obligaciones de protección de datos descritas en el Artículo 28 (3) del RGPD, como se describe en esta Enmienda de procesamiento de datos, se imponen al Subencargado del tratamiento; y

B. seguirá siendo plenamente responsable de todas las obligaciones subcontratadas y de todos los actos y omisiones del Subprocesador.

11.4 Oportunidad de oponerse a los cambios del subprocesador.

A. Cuando se contrata a un nuevo subprocesador de terceros durante el Plazo aplicable, Google, al menos 30 días antes de que el nuevo subprocesador de terceros comience a procesar los datos del cliente, notificará al cliente sobre el compromiso (incluido el nombre y la ubicación del subprocesador correspondiente y las actividades). funcionará).

B. El Cliente puede, dentro de los 90 días posteriores a la notificación de la contratación de un nuevo subprocesador externo, objetar rescindiendo el Acuerdo aplicable inmediatamente notificando a Google. Este derecho de rescisión es el único y exclusivo recurso del Cliente si el Cliente se opone a cualquier nuevo subprocesador de terceros.

12. Equipo de protección de datos en la nube; Procesamiento de registros

12.1 Equipo de protección de datos en la nube de Google. Los administradores del cliente pueden ponerse en contacto con el equipo de protección de datos en la nube de Google en https://support.google.com/a/contact/googlecloud_dpr (mientras los administradores hayan iniciado sesión en su cuenta de administrador) y / o por el cliente proporcionando un aviso a Google como descrito en el Acuerdo aplicable.

12.2. Registros de procesamiento de Google. En la medida en que el GDPR requiera que Google recopile y mantenga registros de cierta información relacionada con el Cliente, el Cliente, cuando se le solicite, utilizará la Consola de administración para proporcionar dicha información y mantenerla precisa y actualizada. Google puede poner dicha información a disposición de las autoridades supervisoras si así lo requiere el RGPD.

13. Responsabilidad

13.1 Límite de responsabilidad. Si las Cláusulas del contrato modelo se han celebrado como se describe en la Sección 10.2 (Transferencias de datos), entonces, sujeto a la Sección 13.2 (Exclusiones del límite de responsabilidad), la responsabilidad total combinada de cualquiera de las partes y sus Afiliadas hacia la otra parte y sus Afiliadas bajo o en relación con el Acuerdo aplicable y dichas Cláusulas de contrato modelo combinadas se limitarán al Límite de responsabilidad acordado para la parte correspondiente.

13.2 Exclusiones del límite de responsabilidad. Nada en la Sección 13.1 (Límite de responsabilidad) afectará los términos restantes del Acuerdo aplicable relacionados con la responsabilidad (incluidas las exclusiones específicas de cualquier limitación de responsabilidad).

14. Tercero beneficiario

Sin perjuicio de cualquier disposición en contrario en el Acuerdo aplicable, cuando Google LLC no sea parte de dicho Acuerdo, Google LLC será un tercero beneficiario de las Secciones 7.5 (Revisiones y auditorías de cumplimiento), 10.2 (Transferencias de datos), 11.1 (Consentimiento para Contratación del subprocesador) y 13 (Responsabilidad).

15 Efecto de la enmienda

Sin perjuicio de cualquier disposición en contrario en el Acuerdo aplicable, en la medida de cualquier conflicto o incoherencia entre los términos de esta Enmienda de procesamiento de datos y el resto del Acuerdo aplicable, prevalecerá esta Enmienda de procesamiento de datos. Para mayor claridad, si el Cliente ha celebrado más de un Acuerdo, esta Enmienda de procesamiento de datos modificará cada uno de los Acuerdos por separado.

Apéndice 1: Asunto y detalles del procesamiento de datos
Tema en cuestión

La prestación de los Servicios y TSS por parte de Google al Cliente.

Duración del procesamiento

El Plazo aplicable más el período desde la expiración de dicho Plazo hasta la eliminación de todos los Datos del Cliente por parte de Google de acuerdo con la Enmienda de Procesamiento de Datos.

Naturaleza y finalidad del tratamiento

Google procesará los Datos personales del cliente con el fin de proporcionar los Servicios y TSS al Cliente de acuerdo con la Enmienda de procesamiento de datos.

Categorías de datos

Datos relacionados con individuos proporcionados a Google a través de los Servicios, por (o bajo la dirección de) el Cliente o los Usuarios finales.

Sujetos de los datos

Los sujetos de los datos incluyen las personas sobre las que se proporcionan datos a Google a través de los Servicios por (o bajo la dirección de) el Cliente o los Usuarios finales.

Apéndice 2: Medidas de seguridad
A partir de la Fecha de entrada en vigor de la Enmienda, Google implementará y mantendrá las Medidas de seguridad descritas en este Apéndice 2.

1. Centro de datos y seguridad de la red
(a) Centros de datos.
Infraestructura. Google mantiene centros de datos distribuidos geográficamente. Google almacena todos los datos de producción en centros de datos físicamente seguros.

Redundancia. Los sistemas de infraestructura se han diseñado para eliminar puntos únicos de falla y minimizar el impacto de los riesgos ambientales anticipados. Los circuitos duales, conmutadores, redes u otros dispositivos necesarios ayudan a proporcionar esta redundancia. Los Servicios están diseñados para permitir que Google realice ciertos tipos de mantenimiento preventivo y correctivo sin interrupción. Todos los equipos e instalaciones ambientales tienen procedimientos de mantenimiento preventivo documentados que detallan el proceso y la frecuencia del desempeño de acuerdo con las especificaciones internas o del fabricante. El mantenimiento preventivo y correctivo del equipo del centro de datos se programa a través de un proceso de cambio estándar de acuerdo con los procedimientos documentados.

Poder. Los sistemas de energía eléctrica del centro de datos están diseñados para ser redundantes y fáciles de mantener sin afectar las operaciones continuas, las 24 horas del día, los 7 días de la semana. En la mayoría de los casos, se proporciona una fuente de energía primaria y otra alternativa, cada una con la misma capacidad, para los componentes de infraestructura críticos en

el centro de datos. La energía de respaldo es proporcionada por varios mecanismos, como las baterías de fuentes de alimentación ininterrumpida (UPS), que brindan protección de energía confiable y constante durante caídas de tensión, apagones, sobrevoltaje, bajo voltaje y condiciones de frecuencia fuera de tolerancia. Si se interrumpe la energía de la red pública, la energía de respaldo está diseñada para proporcionar energía transitoria al centro de datos, a plena capacidad, durante un máximo de 10 minutos hasta que los sistemas de generadores diésel se hagan cargo. Los generadores diésel son capaces de arrancar automáticamente en cuestión de segundos para proporcionar suficiente energía eléctrica de emergencia para hacer funcionar el centro de datos a plena capacidad, normalmente durante varios días.

Sistemas operativos de servidor. Los servidores de Google utilizan una implementación basada en Linux personalizada para el entorno de la aplicación. Los datos se almacenan utilizando algoritmos patentados para aumentar la seguridad y la redundancia de los datos. Google emplea un proceso de revisión de código para aumentar la seguridad del código utilizado para proporcionar los Servicios y mejorar los productos de seguridad en los entornos de producción.

Continuidad de negocios. Google ha diseñado, planifica y prueba periódicamente sus programas de planificación de la continuidad empresarial y recuperación ante desastres.

(b) Redes y Transmisión.
Transmisión de datos. Los centros de datos suelen estar conectados a través de enlaces privados de alta velocidad para proporcionar una transferencia de datos rápida y segura entre los centros de datos. Esto está diseñado para evitar que los datos se lean, copien, alteren o eliminen sin autorización durante la transferencia o transporte electrónico o mientras se graban en medios de almacenamiento de datos. Google transfiere datos a través de protocolos estándar de Internet.

Superficie de ataque externa. Google emplea múltiples capas de dispositivos de red y detección de intrusos para proteger su superficie de ataque externa. Google considera los posibles vectores de ataque e incorpora tecnologías apropiadas diseñadas específicamente en los sistemas externos.

Detección de intrusiones. La detección de intrusiones tiene como objetivo proporcionar información sobre las actividades de ataque en curso y proporcionar información adecuada para responder a los incidentes. La detección de intrusos de Google implica:

1. controlar estrictamente el tamaño y la composición de la superficie de ataque de Google mediante medidas preventivas;
2. emplear controles de detección inteligentes en los puntos de entrada de datos; y
3. emplear tecnologías que resuelvan automáticamente determinadas situaciones peligrosas.
Respuesta al incidente. Google supervisa una variedad de canales de comunicación para detectar incidentes de seguridad, y el personal de seguridad de Google reaccionará rápidamente a los incidentes conocidos.

Tecnologías de cifrado. Google hace que el cifrado HTTPS (también conocido como conexión SSL o TLS) esté disponible. Los servidores de Google admiten el intercambio de claves criptográficas Diffie-Hellman de curva elíptica efímera firmado con RSA y ECDSA. Estos métodos de secreto directo perfecto (PFS) ayudan a proteger el tráfico y minimizar el impacto de una clave comprometida o un avance criptográfico.

2. Controles de acceso y sitio.
(a) Controles del sitio.

Operación de seguridad del centro de datos en el sitio. Los centros de datos de Google mantienen una operación de seguridad en el sitio responsable de todas las funciones de seguridad del centro de datos físico las 24 horas del día, los 7 días de la semana. El personal de operaciones de seguridad en el lugar monitorea las cámaras de circuito cerrado de TV (CCTV) y todos los sistemas de alarma. El personal de operaciones de seguridad in situ realiza patrullas internas y externas del centro de datos con regularidad.

Procedimientos de acceso al centro de datos. Google mantiene un procedimiento de acceso formal para permitir el acceso físico a los centros de datos. Los centros de datos están alojados en instalaciones que requieren acceso con clave de tarjeta electrónica, con alarmas que están vinculadas a la operación de seguridad en el sitio. Todos los que ingresan al centro de datos deben identificarse y mostrar una prueba de identidad para las operaciones de seguridad en el sitio. Solo los empleados, contratistas y visitantes autorizados pueden ingresar a los centros de datos. Solo los empleados y contratistas autorizados pueden solicitar acceso con clave de tarjeta electrónica a estas instalaciones. Las solicitudes de acceso a la clave de la tarjeta electrónica del centro de datos deben realizarse por correo electrónico y requieren la aprobación del gerente del solicitante y del director del centro de datos. Todos los demás participantes que requieran acceso temporal al centro de datos deben: (i) obtener la aprobación previa de los gerentes del centro de datos para el centro de datos específico y las áreas internas que desean visitar; (ii) registrarse en las operaciones de seguridad en el sitio; y (iii) hacer referencia a un registro de acceso al centro de datos aprobado que identifique a la persona como aprobada.

Dispositivos de seguridad del centro de datos en el sitio. Los centros de datos de Google emplean una llave de tarjeta electrónica y un sistema de control de acceso biométrico que está vinculado a un sistema de alarma. El sistema de control de acceso monitorea y registra la llave de la tarjeta electrónica de cada individuo y cuándo acceden a las puertas perimetrales, el envío y la recepción, y otras áreas críticas. El sistema de control de acceso registra la actividad no autorizada y los intentos fallidos de acceso y los investiga, según corresponda. El acceso autorizado en todas las operaciones comerciales y los centros de datos está restringido según las zonas y las responsabilidades laborales de la persona. Las puertas cortafuegos de los centros de datos están alarmadas. Las cámaras de circuito cerrado de televisión están en funcionamiento tanto dentro como fuera de los centros de datos. El posicionamiento de las cámaras ha sido diseñado para cubrir áreas estratégicas que incluyen, entre otras, el perímetro, las puertas al edificio del centro de datos y el envío / recepción. El personal de operaciones de seguridad en el sitio administra el equipo de monitoreo, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan el equipo de CCTV. Las cámaras graban en el sitio a través de grabadoras de video digitales las 24 horas del día, los 7 días de la semana. Los registros de vigilancia se conservan hasta por 30 días según la actividad.

(b) Control de acceso.
Personal de seguridad de infraestructura. Google tiene y mantiene una política de seguridad para su personal y requiere capacitación en seguridad como parte del paquete de capacitación para su personal. El personal de seguridad de la infraestructura de Google es responsable del monitoreo continuo de la infraestructura de seguridad de Google, la revisión de los Servicios y la respuesta a los incidentes de seguridad.

Control de acceso y gestión de privilegios. Los Administradores del Cliente y los Usuarios finales deben autenticarse mediante un sistema de autenticación central o mediante un sistema de inicio de sesión único para poder utilizar los Servicios.

Procesos y políticas de acceso a datos internos - Política de acceso. Los procesos y las políticas de acceso a datos internos de Google están diseñados para evitar que personas o sistemas no autorizados accedan a los sistemas utilizados para procesar datos personales. Google diseña sus sistemas para: (i) permitir que solo las personas autorizadas accedan a los datos a los que están autorizados a acceder; y (ii) garantizar que los datos personales no se puedan leer, copiar, alterar o eliminar sin autorización durante el procesamiento, uso y después de la grabación. Los sistemas están diseñados para detectar cualquier acceso inadecuado. Google emplea un sistema de administración de acceso centralizado para controlar el acceso del personal a los servidores de producción y solo brinda acceso a un número limitado de personal autorizado. Los sistemas de autenticación y autorización de Google utilizan certificados SSH y claves de seguridad, y están diseñados para proporcionar a Google mecanismos de acceso seguros y flexibles. Estos mecanismos están diseñados para otorgar solo derechos de acceso aprobados a los hosts del sitio, los registros, los datos y la información de configuración. Google requiere el uso de ID de usuario únicos, contraseñas seguras, autenticación de dos factores y listas de acceso cuidadosamente monitoreadas para minimizar el potencial de uso no autorizado de la cuenta. La concesión o modificación de derechos de acceso se basa en: las responsabilidades laborales del personal autorizado; requisitos de tareas laborales necesarios para realizar tareas autorizadas; y una necesidad de conocer la base. La concesión o modificación de los derechos de acceso también debe realizarse de acuerdo con las políticas y la formación de acceso a datos internos de Google. Las aprobaciones se gestionan mediante herramientas de flujo de trabajo que mantienen registros de auditoría de todos los cambios. El acceso a los sistemas se registra para crear una pista de auditoría para la rendición de cuentas. Cuando se emplean contraseñas para la autenticación (por ejemplo, inicio de sesión en estaciones de trabajo), se implementan políticas de contraseñas que siguen al menos las prácticas estándar de la industria. Estos estándares incluyen restricciones sobre la reutilización de contraseñas y suficiente seguridad de contraseñas. Para acceder a información extremadamente sensible (por ejemplo, datos de tarjetas de crédito), Google usa identificadores de hardware.

3. Datos

(a) Almacenamiento, aislamiento y registro de datos.

Google almacena datos en un entorno de múltiples inquilinos en servidores propiedad de Google. Sujeto a las instrucciones del Cliente en sentido contrario (por ejemplo, en forma de una selección de ubicación de datos), Google replica los Datos del Cliente entre varios centros de datos dispersos geográficamente. Google también aísla lógicamente los Datos del cliente y separa lógicamente los datos de cada Usuario final de los datos de otros Usuarios finales, y los datos de un Usuario final autenticado no se mostrarán a otro Usuario final (a menos que el Usuario final anterior o un Administrador permita que los datos ser compartido).

El cliente tendrá control sobre políticas específicas de intercambio de datos. Esas políticas, de acuerdo con la funcionalidad de los Servicios, permitirán al Cliente determinar la configuración de uso compartido de productos aplicable a los Usuarios finales para fines específicos. El Cliente puede optar por utilizar la función de registro que Google pone a disposición a través de los Servicios.

(b) Discos retirados y política de borrado de disco.

Los discos que contienen datos pueden experimentar problemas de rendimiento, errores o fallas de hardware que los lleven a ser dados de baja ("Disco fuera de servicio"). Cada Disco retirado está sujeto a una serie de procesos de destrucción de datos (la "Política de borrado de disco") antes de salir de las instalaciones de Google para su reutilización o destrucción. Los discos dados de baja se borran en un proceso de varios pasos y se verifican completos por al menos dos validadores independientes. Los resultados del borrado se registran con el número de serie del disco retirado para su seguimiento. Finalmente, el Disco retirado borrado se libera al inventario para su

reutilización y redespliegue. Si, debido a una falla de hardware, el disco retirado no se puede borrar, se almacena de forma segura hasta que se pueda destruir. Cada instalación se audita periódicamente para supervisar el cumplimiento de la Política de borrado de disco.

4. Seguridad del personal
El personal de Google debe comportarse de manera coherente con las directrices de la empresa con respecto a la confidencialidad, la ética empresarial, el uso adecuado y los estándares profesionales. Google lleva a cabo verificaciones de antecedentes razonablemente apropiadas en la medida en que lo permita la ley y de acuerdo con la legislación laboral local aplicable y las regulaciones estatutarias.

El personal debe firmar un acuerdo de confidencialidad y debe acusar recibo y cumplimiento de las políticas de privacidad y confidencialidad de Google. El personal recibe formación en seguridad. El personal que maneja los Datos del Cliente debe completar los requisitos adicionales adecuados a su función (por ejemplo, certificaciones). El personal de Google no procesará los Datos del cliente sin autorización.

5. Seguridad del subprocesador.
Antes de incorporar a los subprocesadores, Google lleva a cabo una auditoría de las prácticas de seguridad y privacidad de los subprocesadores para garantizar que los subprocesadores brinden un nivel de seguridad y privacidad apropiado para su acceso a los datos y el alcance de los servicios que están contratados para brindar. Una vez que Google ha evaluado los riesgos presentados por el subprocesador, y sujeto a los requisitos descritos en la Sección 11.3 (Requisitos para la participación del subprocesador) de esta Enmienda de procesamiento de datos, el subprocesador debe suscribir los términos del contrato de seguridad, confidencialidad y privacidad adecuados.