Google for Education

Google Workspace for Education Terms of Service

Last modified: November 16, 2023

New to Google Cloud? A quick overview of Google Cloud's online contracting can be found here.

For translations of this Agreement into other languages, please click here.

If you signed an offline variant of this Agreement for use of the Google Workspace for Education Services under the same Google Workspace for Education Account, the terms below do not apply to you and your offline terms govern your use of the Google Workspace for Education Services.

Se a sua conta para faturamento é no Brasil, por gentileza veja o Termos de Serviço (em português e em inglês), que seráo os Termos aplicáveis à sua utilização da Google Workspace for Education.

お客様の請求先アカウントが日本の場合、お客様のGoogle Workspace for Educationのご利用に対してはこちらの利用規約が適用されます.

These Google Workspace for Education Terms of Service (together, the "Agreement") (formerly known as "G Suite for Education Terms of Service" or "G Suite for Education (Online) Agreement") are entered into by Google and the entity or person agreeing to them ("Customer") and govern Customer's access to and use of the Services. "Google" has the meaning given at https://cloud.google.com/terms/google-entity.

This Agreement is effective when Customer clicks to accept it (the "Effective Date"). If you are accepting on behalf of Customer, you represent and warrant that (i) you have full legal authority to bind Customer to this Agreement; (ii) you have read and understand this Agreement; and (iii) you agree, on behalf of Customer, to this Agreement.

1. **Provision of the Services.**

   1.1 **Services Use**. During the Term, Google will provide the Services in accordance with the Agreement, including the SLA. Customer may use the Services ordered in the applicable Order Form or Reseller Order in accordance with this Agreement.

   1.2 **Admin Console**. Customer will have access to the Admin Console, through which Customer may manage its use of the Services.

   1.3 **Accounts; Verification to Use Services**.

   (a) **Accounts**. Customer must have an Account to use the Services and is responsible for the information it provides to create the Account, the security of its passwords for the Account, and any use of its Account. Google has no obligation to provide multiple accounts to Customer.

   (b) **Verification to Use Services**. Customer must verify a Domain Email Address or a Domain Name to use the Services. If Customer does not have valid permission to use the Domain Email Address or does not own or control the Domain Name, then Google will have no obligation to provide Customer with the Services and may delete the Account without notice.

1.4 **Modifications**.

(a) **To the Services**. Google may make commercially reasonable changes to the Services from time to time. Google will inform Customer if Google makes a material change to the Services that has a material impact on Customer's use of the Services and if Customer has subscribed with Google to be informed about such change.

(b) **To the Agreement**. Google may change the terms of this Agreement from time to time and will post any such changes at https://workspace.google.com/terms/education_terms.html. These changes will only take effect at the beginning of Customer's next Order Term, at which time Customer's continued use of the Services will constitute its acceptance of the changes. This Section 1.4(b) (Modifications to the Agreement) does not apply to changes to URL Terms.

(c) **To the URL Terms**. Google may change the URL Terms from time to time and will notify Customer if any such change is material. Google may notify Customer of material SLA changes via the applicable SLA webpage. Material changes to the URL Terms will become effective 30 days after notice is given, except that (i) materially adverse SLA changes will become effective 90 days after notice is given and (ii) changes applicable to new Services or functionality or the Cloud Data Processing Addendum, or that are required by applicable law, will be effective immediately.

(d) **To the Cloud Data Processing Addendum**. Google may only change the Cloud Data Processing Addendum where such change is required to comply with applicable law, is expressly permitted by the Cloud Data Processing Addendum, or:

(i) is commercially reasonable;

(ii) does not result in a material reduction of the security of the Services;

(iii) does not expand the scope of or remove any restrictions on Google's processing of "Customer Personal Data," as described in the "Scope of Processing" Section of the Cloud Data Processing Addendum; and

(iv) does not otherwise have a material adverse impact on Customer's rights under the Cloud Data Processing Addendum.

If Google makes a material change to the Cloud Data Processing Addendum in accordance with this Section 1.4(d) (Modifications to the Cloud Data Processing Addendum), Google will post the change at the webpage containing the Cloud Data Processing Addendum.

(e) **Discontinuation of Core Services**. Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality.

2. **Payment Terms**. If Fees are applicable to Customer's use of any Services, the terms in this Section 2 (Payment Terms) apply to those Services.

2.1 **Usage Measurement and Billing Options**. On or after the Billing Start Date, Google will invoice Customer in advance for the Monthly Charge or Annual Charge, as applicable according to the Order Form. Google's measurement tools will be used to determine Customer's usage of the Services and any such determination by Google for the purpose of calculating Fees is final.

2.2 **Payment**. Customer will pay all Fees in the currency stated in the invoice. All Fees are due 30 days after the invoice date. Google has no obligation to provide multiple invoices. Payments made via wire transfer must include the bank information provided by Google.

2.3 **Taxes**.

(a) Customer is responsible for any Taxes, and will pay Google for the Services without any reduction for Taxes. If Google is obligated to collect or pay any Taxes, the Taxes will be invoiced to Customer and Customer will pay such Taxes to Google, unless Customer provides Google with a timely and valid tax exemption certificate in respect of those Taxes.

(b) Customer will provide Google with any applicable tax identification information that Google may require under applicable law to ensure its compliance with applicable tax regulations and authorities in applicable jurisdictions. Customer will be liable to pay (or reimburse Google for) any taxes, interest, penalties, or fines arising out of any mis-declaration by Customer.

2.4 **Payment Disputes**. Any payment disputes must be submitted in good faith before the payment due date. If Google, having reviewed the dispute in good faith, determines that certain billing inaccuracies are attributable to Google, Google will not issue a corrected invoice, but will instead issue a credit memo specifying the incorrect amount in the affected invoice. If a disputed invoice has not yet been paid, Google will apply the credit memo amount to the disputed invoice and Customer will be responsible for paying the resulting net balance due on that invoice. Nothing in this Agreement obligates Google to extend credit to any party.

2.5 **Delinquent Payments; Suspension**. Late payments (which, for clarity, do not include amounts subject to a good faith payment dispute submitted before the payment due date) may bear interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) from the payment due date until paid in full. Customer will be responsible for all reasonable expenses (including attorneys' fees) incurred by Google in collecting such delinquent amounts. Further, in the event of any late payment for the Services, Google may Suspend the Services.

2.6 **No Purchase Order Number Required**. Customer is obligated to pay all applicable Fees without any requirement for Google to provide a purchase order number on Google's invoice (or otherwise).

2.7 **Price Revisions**. Google may change the Prices at any time unless otherwise expressly agreed in an addendum or Order Form. Google will notify Customer at least 30 days in advance of any changes. Customer's pricing will change at the beginning of Customer's next Order Term after the 30-day period.

3. **Customer Obligations**.

3.1 **Permitted Uses**. Use of the Services under this Agreement is permitted only by (a) educational institutions that meet the criteria at https://support.google.com/a/answer/134628 or a successor URL and (b) non-profit entities (as defined under applicable laws).

3.2 **Compliance**. Customer will (a) ensure that Customer and its End Users' use of the Services complies with the Agreement, (b) use commercially reasonable efforts to prevent and terminate any unauthorized use of, or access to, the Services, and (c) promptly notify Google if Customer becomes aware of any unauthorized use of, or access to, the Services, Account, or Customer's password. Google reserves the right to investigate any potential violation of the AUP by Customer, which may include reviewing Customer Data.

3.3 **Privacy**. Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Services, and (b) Google's accessing, storing, and processing of data provided by Customer (including Customer Data) under the Agreement.

3.4 **Restrictions**. Customer will not, and will not allow End Users to, (a) copy, modify, or create a derivative work of the Services; (b) reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any or all of the source code of, the Services (except to the extent such restriction is expressly prohibited by applicable law); (c) sell, resell, sublicense, transfer, or distribute any or all of the Services; or (d) access or use the Services (i) for High Risk Activities; (ii) in violation of the AUP; (iii) in a manner intended to avoid incurring any applicable Fees (including creating multiple Customer Accounts to simulate or act as a single Customer Account or to circumvent Service-specific usage limits or quotas); (iv) to engage in cryptocurrency mining without Google's prior written approval; (v) to place or receive emergency service calls, unless stated otherwise in the Service Specific Terms; (vi) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (vii) in a manner that breaches, or causes the breach of, Export Control Laws; or (viii) to transmit, store, or process health information subject to United States HIPAA regulations, except as permitted by an executed HIPAA BAA.

3.5 **Additional Products and Third-Party Offerings**. Optional Additional Products and Third-Party Offerings may be available for use in conjunction with the Services, and may be enabled or disabled through the Admin Console. Any use of Additional Products is subject to the Additional Product Terms, which are incorporated by reference into the Agreement and which may be updated by Google from time to time. Any use of Third-Party Offerings is subject to separate terms and policies with the relevant service provider. If Customer intends to enable End Users under the age of 18 to access or use any Additional Products or Third-Party Offerings, then Customer will, before allowing any such End User to access or use those products or offerings, obtain parental consent for the collection and use of personal information by (a) the Additional Products, and (b) to the extent required by applicable law, the Third-Party Offerings.

3.6 **Administration of Services**. Customer may specify through the Admin Console one or more Administrators who will have the right to access Admin Accounts. Customer is responsible for (a) maintaining the confidentiality and security of the End User Accounts and associated passwords and (b) any use of the End User Accounts. Customer agrees that Google’s responsibilities do not extend to the internal management or administration of the Services for Customer or any End Users.

3.7 **Abuse Monitoring**. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names, but Google may monitor emails sent to these aliases to allow Google to identify Services abuse.

3.8 **Requesting Additional End User Accounts During Order Term**. Customer may request additional End User Accounts during an Order Term by means of an additional Order Form or Reseller Order or by ordering via the Admin Console. Such additional End User Accounts will have a pro-rated term ending on the last day of the applicable Order Term.

3.9 **Copyright**. Google responds to notices of alleged copyright infringement and terminates the Accounts of repeat infringers in appropriate circumstances as required to maintain safe harbor for online service providers under the U.S. Digital Millennium Copyright Act.

4. **Suspension**.

4.1 **AUP Violations**. If Google becomes aware that Customer's or any End User's use of the Services violates the AUP, Google will notify Customer and request that Customer correct the violation. If Customer fails to correct the violation within 24 hours of Google's request, then Google may Suspend all or part of Customer's use of the Services until the violation is corrected. Suspension of the Services may include removal or unsharing of content that violates the AUP.

4.2 **Other Suspension**. Notwithstanding Section 4.1 (AUP Violations), Google may immediately Suspend all or part of Customer's use of the Services (including use of the underlying Account) if (a) Google reasonably believes Suspension is needed to protect the Services, Google's infrastructure supporting the Services, or any other customer of the Services (or their end users); (b) there is suspected unauthorized third-party access to the Services; (c) Google reasonably believes that immediate Suspension is required to comply with any applicable law; or (d) Customer is in breach of Section 3.4 (Restrictions) or the Service Specific Terms. Google will lift any such Suspension when the circumstances giving rise to the Suspension have been resolved. At Customer's request, Google will, unless prohibited by applicable law, notify Customer of the basis for the Suspension as soon as is reasonably possible. For Suspension of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

5. **Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features Within the Services**.

5.1 **Intellectual Property Rights**. Except as expressly stated in this Agreement, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data, and Google retains all Intellectual Property Rights in the Services.

5.2 **Protection of Customer Data**. Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Without limiting the generality of the preceding sentence, Google will not process Customer Data for Advertising purposes or serve Advertising in the Services. Google has implemented and will maintain technical, organizational, and physical safeguards to protect Customer Data, as further described in the Cloud Data Processing Addendum.

5.3 **Customer Feedback**. At its option, Customer may provide feedback or suggestions about the Services to Google ("Feedback"). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.

5.4 **Using Brand Features Within the Services**. Google will display within the Services only those Customer Brand Features that Customer authorizes by uploading them into the Services. Google will display those Customer Brand Features within designated areas of the web pages displaying the Services to Customer or its End Users. Customer may specify details of this use in the Admin Console. Google may also display Google Brand Features on such web pages to indicate that the Services are provided by Google.

6. **Technical Support Services**. Subject to payment of applicable Fees, Google will provide TSS to Customer during the Term in accordance with the TSS Guidelines. Certain TSS levels include a minimum recurring Fee as described at https://workspace.google.com/terms/tssg.html. If Customer downgrades its TSS level during any calendar month, Google may continue to provide TSS at the same level and for the same TSS Fees as applied before the downgrade for the remainder of that month.

7. **Confidential Information.**

7.1 **Obligations**. The recipient will only use the disclosing party's Confidential Information to exercise the recipient's rights and fulfill its obligations under the Agreement, and will use reasonable care to protect against the disclosure of the disclosing party's Confidential Information. The recipient may disclose Confidential Information only to its Affiliates, employees, agents, or professional advisors ("Delegates") who need to know it and who have agreed in writing (or in the case of professional advisors are otherwise bound) to keep it confidential. The recipient will ensure that its Delegates use the received Confidential Information only to exercise rights and fulfill obligations under this Agreement.

7.2 **Required Disclosure**. Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its Confidential Information, and (b) comply with the other party's reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual.

8. **Term and Termination.**

8.1 **Agreement Term**. The term of this Agreement (the "Term") will begin on the Effective Date and continue until the Agreement is terminated or not renewed as stated in this Section 8 (Term and Termination).

8.2 **Renewal**. At the end of each Order Term, the Services (and any End User Accounts previously subject to Fees) will automatically renew for an additional Order Term of 12 months. If either party does not want the Services to renew, then it must notify the other party to this effect at least 15 days before the end of the then-current Order Term, and this notice of non-renewal will take effect at the end of the then-current Order Term.

8.3 **Termination for Breach**. To the extent permitted by applicable law, either party may terminate this Agreement immediately on written notice if (a) the other party is in material breach of the Agreement and fails to cure that breach within 30 days after receipt of written

notice of the breach, or (b) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within 90 days.

8.4 **Termination for Convenience**. Customer may stop using the Services at any time. Subject to Customer fulfilling all its financial commitments (if applicable) under an Order Form or otherwise under this Agreement (including payment of any and all Fees for the Order Term), Customer may also terminate this Agreement for its convenience at any time on prior written notice.

8.5 **Termination Due to Applicable Law; Violation of Laws**. Google may terminate this Agreement and/or any applicable Order Form immediately on written notice if Google reasonably believes that (a) continued provision of any Service used by Customer would violate applicable law(s) or (b) Customer has violated or caused Google to violate any Anti-Bribery Laws or Export Control Laws.

8.6 **Effect of Termination or Non-Renewal**. If the Agreement is terminated or not renewed, then (a) all rights and access to the Services will cease (including access to Customer Data), unless otherwise described in this Agreement, and (b) any and all Fees owed by Customer to Google are immediately due upon Customer's receipt of the final invoice.

8.7 **No Refunds**. Unless expressly stated otherwise in this Agreement, termination or non renewal under any section of this Agreement (including the Cloud Data Processing Addendum) will not oblige Google to refund any Fees.

9. **Publicity**. Customer may state publicly that it is a Google customer and display Google Brand Features in accordance with the Trademark Guidelines. Google may use Customer's name and Brand Features in online or offline promotional materials of the Services. Each party may use the other party's Brand Features only as permitted in the Agreement. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.

10. **Representations and Warranties**. Each party represents and warrants that (a) it has full power and authority to enter into the Agreement, and (b) it will comply with all laws applicable to its provision, receipt, or use of the Services, as applicable.

11. **Disclaimer**. **Except as expressly provided for in the Agreement, Google does not make and expressly disclaims to the fullest extent permitted by applicable law (a) any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, title, non-infringement, or error-free or uninterrupted use of the Services and (b) any representations about content or information accessible through the Services.**

12. **Limitation of Liability**.

12.1 **Limitation on Indirect Liability. To the extent permitted by applicable law and subject to Section 12.3 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Agreement for any (a) indirect, consequential, special, incidental, or punitive damages or (b) lost revenues, profits, savings, or goodwill.**

12.2 **Limitation on Amount of Liability. Each party's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the greater of (a) $1,000 USD or (b) the Fees Customer paid during the 12 month period before the event giving rise to Liability.**

12.3 **Unlimited Liabilities. Nothing in the Agreement excludes or limits either party's Liability for:**

(a) its fraud or fraudulent misrepresentation;

(b) its obligations under Section 13 (Indemnification);

(c) its infringement of the other party's Intellectual Property Rights;

(d) its payment obligations (if any) under the Agreement; or

(e) matters for which liability cannot be excluded or limited under applicable law.

13. **Indemnification**.

13.1 **Google Indemnification Obligations**. Google will defend Customer and its Affiliates using the Services under Customer's Account and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that any Service or any Google Brand Feature, in each case used in accordance with the Agreement, infringes the third party's Intellectual Property Rights.

13.2 **Customer Indemnification Obligations**. Customer will defend Google and its Affiliates providing the Services and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from (a) any Customer Data or Customer Brand Features or (b) Customer's or an End User's use of the Services in breach of the AUP or Section 3.3 (Restrictions).

13.3 **Exclusions**. Sections 13.1 (Google Indemnification Obligations) and 13.2 (Customer Indemnification Obligations) will not apply to the extent the underlying allegation arises from (a) the indemnified party's breach of the Agreement or (b) a combination of the indemnifying party's technology or Brand Features with materials not provided by the indemnifying party under the Agreement, unless the combination is required by the Agreement.

13.4 **Conditions**. Sections 13.1 (Google Indemnification Obligations) and 13.2 (Customer Indemnification Obligations) are conditioned on the following:

(a) Any indemnified party must promptly notify the indemnifying party in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and cooperate reasonably with the indemnifying party to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 13.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 13.1 (Google Indemnification Obligations) or 13.2 (Customer Indemnification Obligations) (as applicable) will be reduced in proportion to the prejudice.

(b) Any indemnified party must tender sole control of the indemnified portion of the Third-Party Legal Proceeding to the indemnifying party, subject to the following: (i) the indemnified party may appoint its own non-controlling counsel, at its own expense and (ii) any settlement requiring the indemnified party to admit liability, pay money, or take (or refrain from taking) any action, will require the indemnified party's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

13.5 **Remedies**.

(a) If Google reasonably believes the Services might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense (i) procure the right for Customer to continue using the Services; (ii) modify the Services to make them non-

infringing without materially reducing their functionality; or (iii) replace the Services with a non-infringing, functionally equivalent alternative.

(b) If Google does not believe the remedies in Section 13.5(a) are commercially reasonable, then Google may Suspend or terminate Customer's use of the impacted Services. If Google terminates the impacted Services, then Google will provide a pro-rata refund of any unearned Fees actually paid by Customer applicable to the period following termination of such Services.

13.6 **Sole Rights and Obligations**. Without affecting any other termination rights of either party and to the extent permitted by applicable law, this Section 13 (Indemnification) states the parties' sole and exclusive remedy under this Agreement for any third-party allegations of Intellectual Property Rights infringement covered by this Section 13 (Indemnification).

14. **Resold Customers**. This Section 14 (Resold Customers) applies only if Customer orders the Services from a Reseller under a Reseller Agreement (such Services, "Resold Services").

14.1 **Applicable Terms**. For the purposes of Resold Services:

(a) Section 2 (Payment Terms) of this Agreement will not apply;

(b) Reseller Fees, if applicable, will be payable directly to the Reseller, and any prices for Resold Services will be solely determined between Reseller and Customer;

(c) Customer will receive any applicable SLA credits from Reseller;

(d) Section 12.2 (Limitation on Amount of Liability) is replaced with "Each party's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the greater of (a) $1,000 USD or (b) the Reseller Fees Customer paid for the Resold Services during the 12 month period before the event giving rise to Liability."

(e) Any renewal(s) of the Services and/or any Reseller Order will be as agreed between Customer and Reseller.

(f) "Order Term," as it is used in the Agreement, means the period of time starting on the Services Start Date or the renewal date (as applicable) for the Resold Services and continuing for the period indicated on the then-current Reseller Order unless terminated in accordance with the Agreement; and

(g) "Services Start Date," as it is used in the Agreement, means either the start date described in the Reseller Order or, if none is specified in the Reseller Order, the date Google makes the Resold Services available to Customer.

14.2 **Sharing Confidential Information**. Google may share Customer Confidential Information with Reseller as a Delegate subject to Section 7.1 (Obligations).

14.3 **Reseller as Administrator**. At Customer's discretion, Reseller may access Customer's Account or End User Accounts. As between Google and Customer, Customer is solely responsible for (a) any access by Reseller to Customer's Account or End User Accounts and (b) defining in the Reseller Agreement any rights or obligations as between Reseller and Customer with respect to the Resold Services.

14.4 **Reseller Technical Support**. Customer acknowledges and agrees that Reseller may disclose End User personal data to Google as reasonably required in order for Reseller to handle any support issues that Customer escalates to or via Reseller.

15. **Miscellaneous**.

15.1 **Notices**. Under the Agreement, notices to Customer must be sent to the Notification Email Address and notices to Google must be sent to legal-notices@google.com. Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.

15.2 **Emails**. The parties may use emails to satisfy written approval and consent requirements under the Agreement.

15.3 **Assignment**. Neither party may assign any part of this Agreement without the written consent of the other, except to an Affiliate where (a) the assignee has agreed in writing to be bound by the terms of this Agreement, and (b) the assigning party has notified the other party of the assignment. Any other attempt to assign is void. If Customer assigns this Agreement to an Affiliate in another jurisdiction such that there is a change in the Google contracting entity as defined at https://cloud.google.com/terms/google-entity: (i) this Agreement is automatically assigned to the new Google contracting entity; and (ii) if the Affiliate's billing account is in Brazil or Japan, the applicable terms of service linked above, and not this Agreement, will apply from the moment of the assignment.

15.4 **Change of Control**. If a party experiences a change of Control other than as part of an internal restructuring or reorganization (for example, through a stock purchase or sale, merger, or other form of corporate transaction), that party will give written notice to the other party within 30 days after the change of Control. If Customer ceases to be a non-profit educational institution or other non-profit entity as described in Section 3.1 (Permitted Uses), Customer will notify Google immediately.

15.5 **Force Majeure**. Neither party will be liable for failure or delay in performance to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.

15.6 **Subcontracting**. Google may subcontract obligations under the Agreement but will remain liable to Customer for any subcontracted obligations.

15.7 **No Agency**. This Agreement does not create any agency, partnership, or joint venture between the parties.

15.8 **No Waiver**. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under this Agreement.

15.9 **Severability**. If any part of this Agreement is invalid, illegal, or unenforceable, the rest of the Agreement will remain in effect.

15.10 **No Third-Party Beneficiaries**. This Agreement does not confer any benefits on any third party unless it expressly states that it does.

15.11 **Equitable Relief**. Nothing in this Agreement will limit either party's ability to seek equitable relief.

15.12 **Governing Law**. ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SERVICES WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING THAT STATE'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

15.13 **Amendments**. Except as stated in Section 1.4(b) (Modifications: To the Agreement), (c) (Modifications: To the URL Terms), or (d) (Modifications: To the Cloud Data Processing Addendum), any amendment to this Agreement after the Effective Date must be in writing, signed by both parties, and expressly state that it is amending this Agreement. For clarity, Google's provision of an updated URL in place of any URL stated in this Agreement will not constitute an amendment to or modification of the terms of the Agreement.

15.14 **Survival**. The following Sections will survive expiration or termination of this Agreement: Section 2 (Payment Terms), Section 5 (Intellectual Property Rights; Protection of Customer Data; Feedback; Using Brand Features within the Services), Section 7 (Confidential Information), Section 8.6 (Effect of Termination or Non-Renewal), Section 11 (Disclaimer), Section 12 (Limitation of Liability), Section 13 (Indemnification), Section 14.1 (Applicable Terms), Section 14.2 (Sharing Confidential Information) and Section 15 (Miscellaneous).

15.15 **Entire Agreement**. This Agreement sets out all terms agreed between the parties and terminates and supersedes any and all other agreements between the parties relating to its subject matter, including any prior versions of this Agreement. In entering into this Agreement, neither party has relied on, and neither party will have any right or remedy based on, any statement, representation, or warranty (whether made negligently or innocently), except those expressly stated in this Agreement. The URL Terms are incorporated by reference into the Agreement. After the Effective Date, Google may provide an updated URL in place of any URL in this Agreement.

15.16 **Conflicting Terms**. If there is a conflict between the documents that make up this Agreement, the documents will control in the following order (of decreasing precedence): the Order Form, the Cloud Data Processing Addendum, the remainder of the Agreement (excluding the URL Terms), and the URL Terms (other than the Cloud Data Processing Addendum).

15.17 **Headers**. Headings and captions used in the Agreement are for reference purposes only and will not have any effect on the interpretation of the Agreement.

15.18 **Conflicting Languages**. If this Agreement is translated into any language other than English, and there is a discrepancy between the English text and the translated text, the English text will govern unless expressly stated otherwise in the translation.

15.19 **Definitions**.

- "Account" means Customer's Google account credentials and correlating access to the Services under this Agreement.
- "Additional Products" means products, services, or applications offered by Google or its affiliates that are not incorporated into the Services but that may be accessible for use in conjunction with the Services.
- "Additional Product Terms" means the then-current terms stated at https://workspace.google.com/terms/additional_services.html.
- "Admin Account" means a type of End User Account that Customer (or Reseller, if applicable) may use to administer the Services.
- "Admin Console" means the online console(s) or dashboard provided by Google to Customer for administering the Services.

- "Administrators" mean the Customer-designated personnel who administer the Services to End Users on Customer's behalf, and have the ability to access Customer Data and End User Accounts. Such access includes the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.
- "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 the "Google Sites" functionality within the Services).
- "Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.
- "Annual Charge" means the annual charge for the Services as stated in the Order Form.
- "Anti-Bribery Laws" means all applicable commercial and public anti-bribery laws, including the U.S. Foreign Corrupt Practices Act of 1977 and the UK Bribery Act 2010, that prohibit corrupt offers of anything of value, either directly or indirectly, to anyone, including government officials, to obtain or keep business or to secure any other improper commercial advantage. Government officials include: any government employees, candidates for public office, members of royal families, and employees of government-owned or government-controlled companies, public international organizations, and political parties.
- "AUP" means the then-current acceptable use policy for the Services stated at https://workspace.google.com/terms/use_policy.html.
- "BAA" or "Business Associate Agreement" is an amendment to the Agreement covering the handling of Protected Health Information (as defined in HIPAA).
- "Billing Start Date" means the date from which Google will charge Fees for the Services (if applicable).
- "Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.
- "Cloud Data Processing Addendum" means the then-current terms describing data processing and security obligations with respect to Customer Data, as described at https://cloud.google.com/terms/data-processing-addendum.
- "Confidential Information" means information that one party (or an Affiliate) discloses to the other party under this Agreement, and that is marked as confidential or would normally under the circumstances be considered confidential information. It does not include information that is independently developed by the recipient, is rightfully given to the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient. Subject to the preceding sentence, Customer Data is considered Customer's Confidential Information.
- "Control" means control of greater than 50 percent of the voting rights or equity interests of a party.

- "Core Services" means the then-current "Core Services" as described in the Services Summary, excluding any Third-Party Offerings.
- "Customer Data" means data submitted, stored, sent or received via the Services by Customer or its End Users.
- "Domain Email Address" means the email address on the Domain Name for use in connection with the Services.
- "Domain Name" means the domain name specified in the Order Form or Reseller Order to be used in connection with the Services.
- "End Users" means the individuals who are permitted by Customer to use the Services and managed by an Administrator. For clarity, End Users may include employees of Customer Affiliates and other third parties.
- "End User Account" means a Google-hosted account established by Customer through the Services in order for an End User to use the Services.
- "Export Control Laws" means all applicable export and re-export control laws and regulations, including (a) the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, (b) trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control, and (c) the International Traffic in Arms Regulations ("ITAR") maintained by the U.S. Department of State.
- "Fees" means (a) the product of the amount of the Services used or ordered by Customer multiplied by the Prices (if applicable) or (b) the applicable fees for TSS, plus any applicable Taxes.
- "Help Center" means the Google help center accessible at https://www.google.com/support/.
- "High Risk Activities" means activities where the use or failure of the Services would reasonably be expected to lead to death, personal injury, or environmental or property damage (such as the creation or operation of nuclear facilities, air traffic control, life support systems, or weaponry).
- "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, and any regulations issued under it.
- "including" means including but not limited to.
- "Indemnified Liabilities" means any (i) settlement amounts approved by the indemnifying party and (ii) damages and costs finally awarded against the indemnified party by a court of competent jurisdiction.
- "Intellectual Property Rights" means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.
- "Legal Process" means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, or other valid legal authority, legal procedure, or similar process.
- "Liability" means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.

- "Monthly Charge" means the monthly charge for the Services as stated in the Order Form.
- "Notification Email Address" means the email address(es) designated by Customer in the Admin Console.
- "Order Form" means an order form executed by Customer, or an order placed by Customer via a Google website, in either case specifying the Services Google will provide to Customer under the Agreement.
- "Order Term" means the period of time starting on the Services Start Date or the renewal date (as applicable) and continuing for the period indicated on the Order Form unless terminated in accordance with this Agreement. If no Order Form applies to the Services, the initial Order Term is the term that begins on the Effective Date and continues for 12 months.
- "Other Services" means the then-current "Other Services" as described in the Services Summary, excluding any Third-Party Offerings.
- "Prices" means the then-current applicable prices for the Services described at https://workspace.google.com/pricing.html (incorporated into the Agreement by this reference), unless otherwise agreed in an addendum or Order Form. Prices do not include Taxes.
- "Reseller" means, if applicable, the authorized unaffiliated third party reseller that sells or supplies the Services to Customer.
- "Reseller Agreement" means, if applicable, the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of this Agreement.
- "Reseller Fees" means the fees (if any) for Services used or ordered by Customer as agreed in a Reseller Agreement, plus any applicable Taxes.
- "Reseller Order" means, if applicable, an order form (including a renewal order form) issued by a Reseller and executed by Customer and the Reseller specifying the Services Customer is ordering from the Reseller.
- "Service Specific Terms" means the then-current terms specific to one or more Services stated at https://workspace.google.com/terms/service-terms/.
- "Services" means those Core Services and Other Services included in the then-current applicable Google Workspace for Education edition of the Services.
- "Services Start Date" means either the start date stated in the Order Form or, if none is specified in the Order Form, the date Google makes the Services available to Customer.
- "Services Summary" means the then-current description set out at https://workspace.google.com/terms/user_features.html.
- "SLA" means the then-current service level agreement(s) at https://workspace.google.com/terms/sla.html.
- "Suspend" or "Suspension" means disabling access to or use of the Services or components of the Services.

- "Taxes" means all government-imposed taxes, except for taxes based on Google's net income, net worth, asset value, property value, or employment.
- "Term" has the meaning stated in Section 8.1 (Agreement Term) of this Agreement.
- "Third-Party Legal Proceeding" means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any appellate proceeding).
- "Third-Party Offerings" means third-party services, software, products, and other offerings that are not incorporated into the Services.
- "Trademark Guidelines" means Google's then-current Guidelines for Third Party Use of Google Brand Features at https://www.google.com/permissions/guidelines.html.
- "TSS" means the then-current Google technical support service.
- "TSS Guidelines" means Google's then-current guidelines for technical support services, as stated at https://workspace.google.com/terms/tssg.html.
- "URL Terms" means, collectively, the AUP, Cloud Data Processing Addendum, Service Specific Terms, SLA, and TSS Guidelines.

16. **Region-Specific Terms**. Customer agrees to the following modifications to the Agreement if Customer's billing address is in the applicable region as described below:

Asia Pacific - All regions

Section 2.3 (Taxes) is replaced as follows:

2.3 Taxes. Google will itemize any invoiced Taxes. If Taxes must be withheld from any payment to Google, then Customer will increase the payment to Google so that the net amount received by Google is equal to the amount invoiced, without reduction for Taxes.

The definition of "Taxes" under Section 15.19 (Definitions) is replaced as follows:

15.19 Definitions.

"Taxes" means all government-imposed taxes, as per the applicable law associated with the rendering and performance of the Services, including but not limited to any duties, customs duties, and any direct or indirect taxes, including any related penalties or interest, except for taxes based on Google's profit.

Asia Pacific (all regions excluding Australia, Japan, India, New Zealand, Singapore) and Latin America (all regions excluding Brazil)

Section 15.12 (Governing Law) is replaced as follows:

15.12 Governing Law; Arbitration.

(a) ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY RELATED GOOGLE PRODUCTS OR SERVICES (INCLUDING ANY DISPUTE REGARDING THE INTERPRETATION OR PERFORMANCE OF THE AGREEMENT) ("Dispute") WILL BE GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, USA, EXCLUDING CALIFORNIA'S CONFLICTS OF LAWS RULES.

(b) The parties will try in good faith to settle any Dispute within 30 days after the Dispute arises. If the Dispute is not resolved within 30 days, it must be resolved by arbitration by the American Arbitration Association's International Centre for

Dispute Resolution in accordance with its Expedited Commercial Rules in force as of the date of this Agreement ("Rules").

(c) The parties will mutually select one arbitrator. The arbitration will be conducted in English in Santa Clara County, California, USA.

(d) Either party may apply to any competent court for injunctive relief necessary to protect its rights pending resolution of the arbitration. The arbitrator may order equitable or injunctive relief consistent with the remedies and limitations in the Agreement.

(e) Subject to the confidentiality requirements in Subsection (g), either party may petition any competent court to issue any order necessary to protect that party's rights or property; this petition will not be considered a violation or waiver of this governing law and arbitration section and will not affect the arbitrator's powers, including the power to review the judicial decision. The parties stipulate that the courts of Santa Clara County, California, USA, are competent to grant any order under this Subsection 15.12 (e).

(f) The arbitral award will be final and binding on the parties and its execution may be presented in any competent court, including any court with jurisdiction over either party or any of its property.

(g) Any arbitration proceeding conducted in accordance with this Section 15.12 (Governing Law; Arbitration) will be considered Confidential Information under Section 7 (Confidential Information), including: (i) the existence of, (ii) any information disclosed during, and (iii) any oral communications or documents related to, the arbitration proceedings. In addition to the disclosure rights under Section 7 (Confidential Information), the parties may disclose the information described in this Subsection 15.12 (g) to a competent court as may be necessary to file any order under Subsection 15.12 (e) or execute any arbitral decision, but the parties must request that those judicial proceedings be conducted in camera (in private).

(h) The parties will pay the arbitrator's fees, the arbitrator's appointed experts' fees and expenses, and the arbitration center's administrative expenses in accordance with the Rules. In its final decision, the arbitrator will determine the non-prevailing party's obligation to reimburse the amount paid in advance by the prevailing party for these fees.

(i) Each party will bear its own lawyers' and experts' fees and expenses, regardless of the arbitrator's final decision regarding the Dispute.

Asia Pacific - India

Google India Private Limited has been appointed by Google Asia Pacific Pte. Ltd. ('GAP') as a non-exclusive reseller of the Services (as defined below) in India. For avoidance of any doubts, whilst in the Agreement, both the entities have been referred to as 'Google.' It is hereby clarified that wherever the provisions refer to Google for sales or rights and obligations in relation thereto (including any terms relating to invoicing for sale of services, credit limit, termination of this Agreement, etc.), 'Google' shall mean Google

India Private Limited, and wherever in the Agreement, the provisions refer to 'Google' as a provider of the Services or rights and obligations in relation thereto shall mean 'GAP.'

Google India Private Limited may execute Order Form(s) referencing the Agreement, but the Order Form will form a separate contract between Google India Private Limited and the Customer, and incorporate all of the terms of this Agreement. As a reseller of Services, Google India Private Limited purchases the Services from GAP for resale to the Customer, the entire obligation to provide such Services under the Agreement will be met by GAP and as such, Google India Private Limited will not have any obligation related to performance of Services.

Section 2 (Payment Terms) is replaced as follows:

2. Payment Terms.

2.1 Usage Measurement and Billing Options. Google's measurement tools will be used to determine Customer's usage of the Services and any such determination by Google for the purpose of calculating Fees is final. Customer may elect one of the billing options below or any other option offered by Google when Customer places its order for the Services.

(a) Flexible Plan. If Customer selects this option, Customer will not be committed to purchase the Services for a pre-defined term, but will pay Fees based on its daily usage of the Services, billed monthly in arrears. Any partial day of Services usage will be rounded up to a full day of Services usage for the purposes of calculating Fees.

(b) Annual/Fixed-Term Plan. If Customer selects this option, Customer will be committed to purchasing the Services for one or more annual terms (as selected by Customer). Google will bill Customer according to the terms associated with Customer's elections on the Order Form.

Google may change its offering of billing options (including by limiting or ceasing to offer any billing option) upon 30 days' notice to Customer and any such change will take effect at the beginning of Customer's next Order Term. Billing options may not be available to all customers. Customer may pay for the Services using the payment options listed in Section 2.2 (Payment) below.

2.2 Payment. All payments are due in the currency stated on the Order Form or invoice.

(a) Credit Card or Debit Card. If Customer is paying with a credit card, debit card, or other non-invoice form of payments are due at the end of the month during which Customer received the Services. For credit cards or debit cards, as applicable: (i) Google will issue an electronic bill for all applicable Fees when due, and (ii) these Fees are considered overdue 60 days after the end of the month during which Customer received the Services.

(b) Invoices. Payments for invoices are due 60 days after the invoice date (unless otherwise specified on the Order Form) and are considered overdue after such date.

(c) Other Forms of Payment. Customer may change its payment method to any other method that Google may enable in the Admin Console, subject to

acceptance by Customer of any additional terms applicable to that payment method.

(d) Payment Information. Payments made via wire transfer must include the bank information provided by Google.

2.3 Taxes.

(a) In consideration of services, Customer agrees to pay to Google, the Fees as mentioned above plus applicable Taxes. If Google is obligated to collect or pay Taxes, the Taxes will be invoiced to Customer, unless Customer provides Google with a timely and valid tax exemption certificate authorized by the appropriate taxing authority.

(b) If required under applicable law, Customer will provide Google with applicable tax identification information (Goods and Services Tax Identification Number ("GSTIN"), location where the services would be received by the customer, tax status etc.) that Google may require to ensure its compliance with applicable tax regulations in India. The Customer acknowledges that all the details provided such as the GSTIN, location where the services would be received by the customer, tax status etc. are correct. The address and GSTIN provided are of the location where the services would be received by the Customer. Customer will be liable to pay (or reimburse Google for) any taxes, interest, penalties or fines arising out of any mis-declaration by the Customer.

(c) If Customer is required by law to withhold any amounts for Income Tax on its payments to Google, Customer must provide Google in a timely manner with a withholding tax certificate or other appropriate documentation to support such withholding as per the applicable tax laws.

2.4 Payment Disputes. Any payment disputes must be submitted before the payment due date. If the parties determine that certain billing inaccuracies are attributable to Google, Google will not issue a corrected invoice, but will instead issue a credit memo specifying the incorrect amount in the affected invoice. If a disputed invoice has not yet been paid, Google will apply the credit memo amount to the disputed invoice and Customer will be responsible for paying the resulting net balance due on that invoice. Nothing in this Agreement obligates Google to extend credit to any party.

2.5 Delinquent Payments; Suspension. Late payments may bear interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) from the payment due date until paid in full. Customer will be responsible for all reasonable expenses (including attorneys' fees) incurred by Google in collecting such delinquent amounts. Further, if Customer’s payment for the Services is overdue, Google may through Google suspend the Services.

2.6 No Purchase Order Number Required. Customer is obligated to pay all applicable Fees without any requirement for Google to provide a purchase order number on Google's invoice (or otherwise).

2.7 Price Revisions. Google may change the Prices at any time unless otherwise expressly agreed in an addendum or Order Form. Google will notify Customer at least 30

days in advance of any changes. Customer's pricing will change at the beginning of Customer's next Order Term after the 30-day period.

Section 15.12 (U.S. Governing Law) is replaced as follows:

15.12 Governing Law. All claims arising out of or related to this Agreement will be governed by the laws of India. In case of any disputes the Courts at New Delhi shall have jurisdiction. Notwithstanding the above, the Customer can and will bring all claims with respect to Google under the Agreement against Google India Private Limited.

The definition of "Taxes" under Section 15.19 (Definitions) is replaced as follows:

15.19 Definitions.

"Taxes" means all taxes as per the applicable law including but not limited to any duties, or taxes (other than income tax), including indirect taxes such as goods and services tax ("GST") or such taxes associated with the purchase of the Services.

Asia Pacific - Indonesia

A new Section 8.8 is added:

8.8 Termination Waiver. The parties agree to waive any provisions under any applicable laws to the extent that a court decision or order is required for the cancellation of this Agreement.

The Indonesian version of this Agreement is accessible here and Section 15.18 (Conflicting Languages) is replaced as follows:

15.18 Conflicting Languages. This Agreement is made in the Indonesian and the English language. Both versions are equally authentic. In the event of any inconsistency or different interpretation between the Indonesian version and the English version, the parties agree to amend the Indonesian version to make the relevant part of the Indonesian version consistent with the relevant part of the English version.

Asia Pacific - Australia

A new Section 11A is added as follows:

11A. This Section 11A applies only if the Services are subject to statutory guarantees under the Australian Competition and Consumer Act 2010 ("ACCA"). Applicable laws, including the ACCA, may confer rights and remedies into this Agreement that cannot be excluded, and which are not excluded by this Agreement. To the extent that the applicable laws permit Google to limit their operation, Google's and its Affiliates' liability under those laws will be limited at its option, to the supply of the Services again, or payment of the cost of having the Services supplied again.

Section 15.12(c) (U.S. Governing Law) is amended by inserting the following text at the end of that Section: "IF APPLICABLE LAW PREVENTS A DISPUTE FROM BEING RESOLVED IN A CALIFORNIA COURT, THEN CUSTOMER MAY FILE THE DISPUTE IN CUSTOMER'S LOCAL COURTS. IF APPLICABLE LAW PREVENTS CUSTOMER'S LOCAL COURT FROM APPLYING CALIFORNIA LAW TO RESOLVE A DISPUTE, THEN THE DISPUTE WILL BE GOVERNED BY THE APPLICABLE LOCAL LAWS OF CUSTOMER'S COUNTRY, STATE, OR OTHER PLACE OF RESIDENCE."

Section 15.15 (Entire Agreement) is amended by inserting the following text at the end of that Section: "Nothing in this Agreement excludes a party's liability for prior written or oral

misrepresentation."

Europe, Middle East, and Africa - All regions

Section 2.2 (Payment) is replaced as follows:

2.2 Payment. Customer will pay all Fees in the currency stated in the invoice. All Fees are due 30 days from the invoice date. Google has no obligation to provide multiple invoices. Payments made via wire transfer must include the bank information provided by Google. If Customer has entered into the Agreement with Google Commerce Limited, Google may collect payments via Google Payment Limited, a company incorporated in England and Wales with offices at Belgrave House, 76 Buckingham Palace Road, London, SW1W 9TQ, United Kingdom.

Europe, Middle East, and Africa - European Economic Area, the United Kingdom, and Switzerland

Section 15.19 (Definitions) is changed to Section 15.20 (Definitions).

A new Section 15.19 is added:

15.19 EECC Waiver.

(a) For the purposes of this Section 15.19 (EECC Waiver), the terms "microenterprise", "small enterprise" and "not-for-profit" will have the meanings in the EECC. "EECC" means the European Electronic Communications Code (as established by Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018).

(b) The parties acknowledge that under the EECC: (i) certain rights extend to microenterprises, small enterprises and not for profits and (ii) customers falling within the categories referred to in (i) can explicitly agree to waive certain rights.

(c) If Customer is a microenterprise, small enterprise or not for profit, Customer agrees to waive any rights it may have under:

(i) Article 102(1) EECC, which allows Customer to receive certain pre-contractual information;

(ii) Article 102(3) EECC, which allows Customer to receive a contract summary;

(iii) Article 105(1) EECC, which limits the maximum contract duration to 24 months for certain services; and

(iv) Article 107(1) EECC, which extends other rights in the EECC (including Articles 102(3) and 105(1) as described above) to all services provided under the same Google Workspace agreement.

Europe, Middle East and Africa - Algeria, Bahrain, Jordan, Kuwait, Libya, Mauritania, Morocco, Oman, Palestine, Qatar, Tunisia, Yemen, Egypt, Israel, United Arab Emirates and Lebanon

A new Section 8.8 is added as follows:

8.8 No requirement for Court Order. Both parties acknowledge and agree that a court order will not be required to give effect to any termination or amendment of the Agreement or to give effect to any other section of the Agreement.

Section 15.12 (Governing Law) is replaced as follows:

15.12 Governing Law; Arbitration.

(a) ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY RELATED GOOGLE PRODUCTS OR SERVICES (INCLUDING ANY DISPUTE REGARDING THE INTERPRETATION OR PERFORMANCE OF THE AGREEMENT) ("Dispute") WILL BE GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, USA, EXCLUDING CALIFORNIA'S CONFLICTS OF LAWS RULES.

(b) The parties will try in good faith to settle any Dispute within 30 days after the Dispute arises. If the Dispute is not resolved within 30 days, it must be resolved by arbitration under the Arbitration Rules of the London Court of International Arbitration (LCIA) ("Rules"), which Rules are deemed to be incorporated by reference to this Section.

(c) The parties will mutually select one arbitrator. The arbitration will be conducted in English and the place and the legal seat of the arbitration will be the Dubai International Financial Center, DIFC, Dubai UAE.

(d) Either party may apply to any competent court for injunctive relief necessary to protect its rights pending resolution of the arbitration. The arbitrator may order equitable or injunctive relief consistent with the remedies and limitations in the Agreement.

(e) The arbitral award will be final and binding on the parties and its execution may be presented in any competent court, including any court with jurisdiction over either party or any of its property.

(f) Any arbitration proceeding conducted in accordance with this Section 15.12 (Governing Law; Arbitration) will be considered Confidential Information under Section 7 (Confidential Information), including: (i) the existence of, (ii) any information disclosed during, and (iii) any oral communications or documents related to, the arbitration proceedings. In addition to the disclosure rights under Section 7 (Confidential Information), the parties may disclose the information described in this Subsection 15.12 (f) to a competent court as may be necessary to execute any arbitral decision, but the parties must request that those judicial proceedings be conducted in camera (in private).

(g) The parties will pay the arbitrator’s fees, the arbitrator's appointed experts' fees and expenses, and the arbitration center's administrative expenses in accordance with the Rules. In its final decision, the arbitrator will determine the non-prevailing party's obligation to reimburse the amount paid in advance by the prevailing party for these fees.

(h) Each party will bear its own lawyers’ and experts’ fees and expenses, regardless of the arbitrator’s final decision regarding the Dispute.

North America - United States and Latin America (all regions excluding Brazil)

A new Section 3.10 is added:

3.10 COPPA and Parental Consent. If Customer allows End Users under the age of 13 to use the Services, Customer consents as required under the Children's Online Privacy Protection Act ("COPPA") to the collection and use of personal information in the Services, described in the Google Workspace for Education Privacy Notice, from such End Users (to the extent COPPA is applicable in Customer's jurisdiction).

A new Section 7.3 is added:

7.3 FERPA. The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA ("FERPA Records") and (b) to the extent that Customer Data includes FERPA Records, Google will be considered a "School Official" (as that term is used in FERPA and its implementing regulations) and will comply with FERPA. "FERPA" means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

Section 15.19 (Definitions) is changed to Section 15.20 (Definitions).

A new Section 15.19 is added:

15.19 Services Development. The Services were developed solely at private expense and are commercial computer software and related documentation within the meaning of the applicable Federal Acquisition Regulations and their agency supplements.

Applicable to Public Educational Institutions only: North America - United States and Latin America (all regions excluding Brazil)

Section 2.5 (Delinquent Payments; Suspension) is replaced as follows:

2.5 Delinquent Payments; Suspension. Late payments may bear interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) starting 30 days from the payment due date until paid in full. Further, if the Customer is late on payment for the Services is overdue, Google may Suspend the Services or terminate the Agreement for breach under Section 8.3 (Termination for Breach).

Section 13.2 (Customer Indemnification Obligations) is replaced as follows:

13.2 Customer Indemnification Obligations. If Google is damaged or becomes subject to a Third-Party Legal Proceeding as a result of Customer's infringement of any third-party intellectual property, Google will pursue available remedies under applicable federal, state, local, or other law.

Section 15.12 (Governing Law) is replaced as follows:

15.12 Governing Law. If Customer is a U.S. city, county, or state government entity, then the Agreement will be silent regarding governing law and venue.

Previous Versions

July 12, 2023

April 19, 2023

March 14, 2023

Feburary 6, 2023

November 7, 2022

September 20, 2022

September 20, 2021

April 1, 2021

February 17, 2021

India (February 17, 2021)

Americas (October 6, 2020)

APAC (October 6, 2020)

EMEA (October 6, 2020)

Google Workspace

GOOGLE WORKSPACE FOR EDUCATION PRIVACY NOTICE

This privacy notice is meant to help you understand what data we collect, why we collect it, and how you can manage your information while using a Google Workspace for Education account.

Contents

Contact Us

Introduction

Google Workspace for Education facilitates learning and collaboration among students (and parents), educators, and school admins. Google Workspace for Education includes two categories of services, both described in this privacy notice. The distinction is important because the scope of the services and how the data is processed in these services differs.

- **Google Workspace for Education core services** are listed in the Services Summary and include Gmail, Calendar, Classroom, Assignments, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Chat, Meet, Vault, and Chrome Sync.

- **Google Workspace for Education additional services** include services we make generally available for all consumers, such as Google Search, Maps, and YouTube, which Workspace for Education users may have access to with their Workspace accounts.

This document provides the key information about both types of services. If you want to learn more, you can find additional information and examples in the following documents that also apply to Google Workspace for Education accounts. The Google Cloud Privacy Notice provides more information about data that we process while providing the core services, and the Google Privacy Policy provides more information about data that we process in additional services. Information provided in this notice relating to core services also applies to Other Services listed in the Services Summary, including AppSheet.

Your information: what we collect & how it's used

A Google Workspace for Education account is a Google Account created and managed by a school for use by students and educators. The account can be used for both core and additional services, and the information that we collect and store in your account is treated as personal information. Admins manage how students use core and additional services with their Google Workspace for Education accounts, including obtaining parental consent for the additional services that they choose to enable for students. Learn more about core and additional services for Google Workspace for Education users.

Core Services

As students, educators, and admins use Workspace core services, we collect two types of data:

- Things that you provide or create through core services (customer data)
- Information we collect as you use core services (service data)

There are no ads shown in Google Workspace for Education core services. Also, none of the personal information collected in the core services is used for advertising purposes.

Things that you provide or create through core services

We receive customer data through the core services and process it according to the school's (the customer's) instructions. This customer data includes anything submitted, stored, sent or received through core services by you or your school.

When a Google Workspace for Education account is created, the school provides Google with certain personal information about its students and educators that includes the user's name, email address, and password. Schools can also choose to share things like a user's secondary email address, phone number, and address. And users can also add information to their account, such as an additional phone number and profile photo.

Things that you might create through the services include emails that you write and receive while using Gmail or documents that you draft and store in Drive.

Customer data is used to provide the core services, for example, Google processes your email address to send and deliver messages between teachers and students.

Information we collect as you use core services

As described fully in Google's Cloud Privacy Notice, we also collect service data through the core services, including:

- **Your account information**, which includes things like name and email address.
- **Your activity while using the core services**, which includes things like viewing and interacting with content, people with whom you communicate or share content, and other details about your usage of the services.
- **Your settings, apps, browsers & devices**. We collect info about your settings and the apps, browsers, and devices you use to access our services. This information includes browser and device type, settings configuration, unique identifiers, operating system, mobile network information, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date and time of your request.
- **Your location information**. We collect info about your location as determined by various technologies such as IP address.
- **Your direct communications**. We keep records of communications when you or your admin provide feedback, ask questions, or seek technical support.
- And for admins, we collect data about payments and transactions.

Service data is primarily used to deliver the services that schools and students use, but it's also used to maintain and improve the services; make recommendations to optimize the use of the services; provide and improve other services you request; provide support; protect our users, customers, the public, and Google; and comply with legal obligations. See the Google Cloud Privacy Notice for more information.

Additional Services

As students, educators, and admins use additional services, we collect two types of data:

- Things that you provide or create through additional services
- Information we collect as you use additional services

Things that you provide or create through additional services

As described more fully in Google's Privacy Policy, we collect information when students and educators use the additional services, including things that you provide to us, content that's created or uploaded, and content that's received from others. For example, if you sign in to an additional service with a Workspace account, we'll use your Workspace name and profile information to identify your account. You can also choose to save your content with Google, things like photos and videos.

Information we collect as you use additional services

Google's Privacy Policy also describes the information we collect as you use our additional services, which includes:

- **Your activity while using additional services**, which includes things like terms you search for, videos you watch, content and ads you view and interact with, voice and audio information when you use audio features, purchase activity, and activity on third-party sites and apps that use our services.
- **Your apps, browsers & devices**. We collect the info about your apps, browser, and devices described above in the core services section.
- **Your location information**. We collect info about your location as determined by various technologies including: GPS, IP address, sensor data from your device, and information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices. The types of location data we collect depend in part on your device and account settings.

Why we collect data

The data we collect in the additional services is used across our services to deliver, maintain, and improve our services; develop new services; provide personalized services; measure performance; communicate with you; and protect Google, our users, and the public. See the Google Privacy Policy for more details.

Some additional services show ads. But if you're using your Google Workspace for Education account in primary and secondary schools (K-12), we don't show you personalized ads, which means we don't use information from your account or past activity to target ads. However, we may show ads based on general factors like your search query, the time of day, or the content of a page you're reading.

Sharing your information

When you share your information

Your school's admin may allow students to access Google services, such as Google Docs and YouTube, that have features that allow users to share information with others or publicly. For example, if you leave a review in Google Play, your name and photo appear next to your activity. And if you share a photo with a friend who then makes a copy of it, or shares it again, then that photo may continue to appear in your friend's Google Account even after you remove it from your Google Account. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When Google shares your information

As described fully in the Google Privacy Policy and the Google Cloud Privacy Notice, we do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

- **With your school's admin**: Your admin and resellers who manage your or your organization's Workspace account will have access to your information. For example, they may be able to:
    - View account information, activity and statistics;
    - Change your account password;
    - Suspend or terminate your account access;
    - Access your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request;
    - Restrict your ability to delete or edit your information or your privacy settings.
- **With your consent**: We'll share personal information outside of Google where we have you or your parent's consent.
- **For external processing**: We share personal information with our affiliates and other trusted third party providers to process it for us as we instruct them and in compliance with our Privacy Policy, the Google Cloud Privacy Notice, and any other appropriate confidentiality and security measures.

- **For legal reasons**: We share personal information outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary for legal reasons, including complying with enforceable governmental requests and protecting you and Google.

Your privacy controls

We provide a variety of controls that enable students and parents to make meaningful choices about how information is used in Google services. Depending on the settings enabled by your school's admin, students can use settings like Google activity controls, to manage their privacy and information. We provide additional information for parents, students, and admins in the Google Workspace for Education Privacy Center.

School admins also have service controls that can allow you to manage personal information, including limiting its further collection or use. If you or your child has a Google Workspace for Education account, contact your admin to:

- access your personal information
- limit access to features or services
- delete personal information in services or delete your entire account

About this policy

This Notice is intended to provide the key information about our collection and use of data for Google Workspace for Education users, and is consistent with the Google Privacy Policy and the Google Cloud Privacy

Notice. In cases that specific commitments differ, this privacy notice takes precedence followed by the Google Cloud Privacy Notice and the Google Privacy Policy. For example, the Google Privacy Policy has a description of personalized ads that isn't relevant to Google Workspace for Education users in primary and secondary schools (K-12), and this notice clarifies that we don't show personalized ads to those students.

Contact Us

Please visit the Google Workspace for Education Privacy Center for answers to most questions. Also see our Privacy Help Center for questions about privacy and Google's services.

If you're a parent:

- Contact your school admin if you have questions regarding the management of Google Workspace for Education accounts or the use of information by your child's school
- Or contact Google about the information in this notice

If you're an admin, contact Google about the information in this Notice by submitting the contact form while signed in to your admin account.

Google

1600 Amphitheatre Parkway

Mountain View, CA 94043, USA

(650) 253-0000

Back to Google Cloud Terms Directory (/product-terms) > Current

Cloud Data Processing Addendum (Customers)

This Cloud Data Processing Addendum (including its appendices, the "*Addendum*") is incorporated into the Agreement(s) (as defined below) between Google and Customer. This Addendum was formerly known as the "Data Processing and Security Terms" under an Agreement for Google Cloud Platform, Looker (original) or Google SecOps Services or the "Data Processing Amendment" under an Agreement for Google Workspace or Cloud Identity.

Table of Contents:

General Terms

1. Overview

This Addendum describes the parties' obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Data (as defined below). This Addendum will be effective on the Addendum Effective Date (as defined below), and will replace any terms previously applicable to the processing and security of Customer Data. Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement.

2. Definitions

2.1 In this Addendum:

- "*Addendum Effective Date*" means the date on which Customer accepted, or the parties otherwise agreed to, this Addendum.
- "*Additional Security Controls*" means security resources, features, functionality, and controls that Customer may use at its option and as it determines, including the Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- "*Agreement*" means the contract under which Google has agreed to provide the applicable Services to Customer.
- "*Applicable Privacy Law*" means, as applicable to the processing of Customer Personal Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation.
- "*Audited Services*" means the then-current Services indicated as being in-scope for the relevant certification or report at https://cloud.google.com/security/compliance/services-in-scope (https://cloud.google.com/security/compliance/services-in-scope). Google may not remove any Services from this URL unless they have been discontinued in accordance with the applicable Agreement.
- "*Compliance Certifications*" has the meaning given in Section 7.4 (Compliance Certifications and SOC Reports).

- "*Customer Data*", if not defined in the Agreement, has the meaning given in Appendix 4 (Specific Products).
- "*Customer Personal Data*" means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.
- "*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.
- "*EMEA*" means Europe, the Middle East and Africa.
- "*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; or (b) the Swiss FADP.
- "*European Law*" means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Personal Data).
- "*GDPR*" means, as applicable: (a) the EU GDPR; 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.
- "*Instructions*" has the meaning given in Section 5.2 (Compliance with Customer's Instructions).
- "*Notification Email Address*" means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Google.
- "*Security Documentation*" means the Compliance Certifications and the SOC Reports.

- "*Security Measures*" has the meaning given in Section 7.1.1 (Google's Security Measures).
- "*Services*" means the applicable services described in Appendix 4 (Specific Products).
- "*SOC Reports*" has the meaning given in Section 7.4 (Compliance Certifications and SOC Reports).
- "*Subprocessor*" means a third party authorized as another processor under this Addendum to 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; or (b) the "Commissioner" as defined in the UK GDPR or the Swiss FADP.
- "*Swiss FADP*" means, as applicable, the Federal Act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).
- "*Term*" means the period from the Addendum Effective Date until the end of Google's provision of the Services, 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, and applicable secondary legislation made under that Act.

2.2 The terms "personal data", "data subject", "processing", "controller", and "processor" as used in this Addendum have the meanings given by Applicable Privacy Law or, absent any such meaning or law, by the EU GDPR.

2.3 The terms "data subject", "controller" and "processor" include "consumer", "business", and "service provider", respectively, as required by Applicable Privacy Law.

3. Duration

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google deletes all Customer Data as described in this Addendum.

4. Roles; Legal Compliance

4.1 *Roles of Parties*. Google is a processor and Customer is a controller or processor, as applicable, of Customer Personal Data.

4.2 *Processing Summary*. The subject matter and details of the processing of Customer Personal Data are described in Appendix 1 (Subject Matter and Details of the Processing).

4.3 *Compliance with Law*. Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Privacy Law.

4.4 *Additional Legal Terms*. To the extent the processing of Customer Personal Data is subject to an Applicable Privacy Law described in Appendix 3 (Specific Privacy Laws), the corresponding terms in Appendix 3 will apply in addition to these General Terms and prevail as described in Section 14.1 (Precedence).

5. Data Processing

5.1 *Processor Customers*. If Customer is a processor:

a. Customer warrants on an ongoing basis that the relevant controller has authorized:

i. the Instructions;

ii. Customer's engagement of Google as another processor; and.

iii. Google's engagement of Subprocessors as described in Section 11 (Subprocessors);

b. Customer will forward to the relevant controller promptly and without undue delay any notice provided by Google under Section 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), or 11.4 (Opportunity to Object to Subprocessors); and

c. Customer may make available to the relevant controller any other information made available by Google under this Addendum about the locations of Google data centers or the names, locations and activities of Subprocessors.

5.2 *Compliance with Customer's Instructions*. Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) and applicable law only as follows:

a. to provide, secure, and monitor the Services and TSS; and

b. as further specified via:

i. Customer's use of the Services (including via the Admin Console) and TSS; and

ii. any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum

(collectively, the "*Instructions*").

Google will comply with the Instructions unless prohibited by European Law, where European Data Protection Law applies, or prohibited by applicable law, where any other Applicable Privacy Law applies.

6. Data Deletion

6.1 *Deletion by Customer*. Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, 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 Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

6.2 *Return or Deletion When Term Ends*. If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google's systems at the end of the Term in accordance with applicable law. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where

European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

6.3. *Deferred Deletion Instruction*. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Return or Deletion When Term Ends) 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 take effect with respect to such Customer Data only when the continuing Term expires. For clarity, this Addendum 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, organizational, and physical measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (Security Measures) *(*the *"Security Measures")*. The Security Measures include measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer 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 a material reduction of the security of the Services.

7.1.2 *Access and Compliance*. Google will:

a. authorize its employees, contractors and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions;

b. 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

c. ensure that all persons authorized to process Customer 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 (or, where Customer is a processor, the relevant controller's) obligations relating to security and personal data breaches under Applicable Privacy Law, 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 in accordance with Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. making the Security Documentation available in accordance with Section 7.5.1 (Reviews of Security Documentation) and providing the information contained in the applicable Agreement (including this Addendum); and

e. if subsections (a)-(d) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and 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: the nature of the Data Incident including the Customer resources impacted; the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Google recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Google's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3 *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.

7.2.4 *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 to the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. backing up or retaining copies of its Customer Data as appropriate.

7.3.2 *Customer's Security Assessment*. Customer agrees that the Services, Security Measures, Additional Security Controls, and Google's commitments under this Section 7 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Data as well as the risks to individuals).

7.4 *Compliance Certifications and SOC Reports*. Google will maintain at least the following for the Audited Services to verify the continued effectiveness of the Security Measures:

a. certificates for ISO 27001 and any additional certifications described in Appendix 4 (Specific Products) (the "*Compliance Certifications*"); 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 Compliance Certification or SOC Report with an equivalent or enhanced alternative.

7.5 *Reviews and Audits of Compliance*.

7.5.1 *Reviews of Security Documentation*. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the Security Documentation available for review by Customer and, if Customer is a processor, allow Customer to request access to the SOC Reports for the relevant controller in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

7.5.2 *Customer's Audit Rights*.

a. *Customer Audit*. Google will, if required under Applicable Privacy Law, allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Addendum in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Google will reasonably cooperate with Customer or its auditor as described in this Section 7.5 (Reviews and Audits of Compliance).

b. *Customer Independent Review*. Customer may conduct an audit to verify Google's compliance with its obligations under this Addendum 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 contact Google's Cloud Data Protection Team to request:

i. access to the SOC Reports for a relevant controller under Section 7.5.1 (Reviews of Security Documentation); or

ii. an audit under Section 7.5.2(a) (Customer Audit).

b. Following a Customer request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on:

i. security and confidentiality controls applicable to any access to the SOC Reports by a relevant controller under Section 7.5.1 (Reviews of Security Documentation); 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) (Customer Audit).

c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) (Customer Audit). 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) (Customer Audit) 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.

e. Any Customer requests under Appendix 3 (Specific Privacy Laws) or Appendix 4 (Specific Products) for access to any SOC reports for a relevant controller or for audits will also be subject to this Section 7.5.3 (Additional Business Terms for Reviews and Audits).

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 (or, where Customer is a processor, the relevant controller's) obligations relating to data protection assessments, risk assessments, prior regulatory consultations or equivalent procedures under Applicable Privacy Law, by:

a. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation available in accordance with Section 7.5.1 (Reviews of Security Documentation);

b. providing the information contained in the applicable Agreement (including this Addendum); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9. Access; Data Subject Rights; Data Export

9.1 *Access; Rectification; Restricted Processing; Portability*. During the 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 by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by Applicable Privacy Law.

9.2 *Data Subject Requests*.

9.2.1 *Responsibility for Requests*. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will:

a. advise the data subject to submit their request to Customer;

b. promptly notify Customer; and

c. not otherwise respond to that data subject's request without authorization from 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 (or, where Customer is a processor, the relevant controller's) obligations under Applicable Privacy Law to respond to requests for exercising the data subject's rights by:

a. making Additional Security Controls available 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 (Responsibility for Requests); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

10. Data Processing Locations

10.1 *Data Storage and Processing Facilities.* Subject to Google's data location commitments under the Service Specific Terms and data transfer commitments under Appendix 3 (Specific Privacy Laws), if applicable, Customer Data may be processed in any country where Google or its Subprocessors maintain facilities.

10.2 *Data Center Information*. The locations of Google data centers are described in Appendix 4 (Specific Products).

11. Subprocessors

11.1 *Consent to Subprocessor Engagement*. Customer specifically authorizes Google's engagement as Subprocessors of those entities disclosed as described in Section 11.2 (Information about Subprocessors) as of the Addendum Effective Date. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessors), Customer generally authorizes Google's engagement of other third parties as Subprocessors ("*New Subprocessors*").

11.2 *Information about Subprocessors*. Names, locations, and activities of Subprocessors are described in Appendix 4 (Specific Products).

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 applicable Agreement (including this Addendum); and

ii. if required under Applicable Privacy Laws, the data protection obligations described in this Addendum are imposed on the Subprocessor (as may be further described in Appendix 3 (Specific Privacy Laws)); and

b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 *Opportunity to Object to Subprocessors*.

a. When Google engages any New Subprocessor during the Term, Google will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location and activities of the New Subprocessor).

b. Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by immediately terminating the applicable Agreement for convenience:

i. in accordance with that Agreement's termination for convenience provision; or

ii. if there is no such provision, by notifying Google.

12. Cloud Data Protection Team; Processing Records

12.1 *Cloud Data Protection Team*. Google's Cloud Data Protection Team will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Data under the applicable Agreement and can be contacted as described in the Notices section of the applicable Agreement or in Appendix 4 (Specific Products).

12.2 *Google's Processing Records*. Google will keep appropriate documentation of its processing activities as required by Applicable Privacy Law. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console or other means identified in Appendix 4 (Specific Products) to supply such information and keep it accurate and up-to-date. Google may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Privacy Law.

12.3 *Controller Requests*. During the Term, if Google's Cloud Data Protection Team receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Google will advise the third party to contact Customer.

13. Notices

Notices under this Addendum (including notifications of any Data Incidents) will be delivered to the Notification Email Address. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.

14. Interpretation

14.1 *Precedence*. To the extent of any conflict between:

a. Appendix 3 (Specific Privacy Laws) and the remainder of the Addendum (including Appendix 4 (Specific Products)), Appendix 3 will prevail; and

b. Appendix 4 (Specific Products) and the remainder of the Addendum (excluding Appendix 3), Appendix 4 will prevail; and

c. this Addendum and the remainder of the Agreement, this Addendum will prevail.

For clarity, if Customer has more than one Agreement, this Addendum will amend each of the Agreements separately.

14.2 *Section References*. Unless indicated otherwise, section references in any Appendix to this Addendum refer to sections of the General Terms of the Addendum.

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 Term plus the period from the end of the Term until deletion of all Customer Data by Google in accordance with this Addendum.

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 this Addendum.

Categories of Data

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

Appendix 2: Security Measures

As from the Addendum 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 backup generator systems take over. The backup 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.

Code Quality. 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: (i) tightly controlling the size and make-up of Google's attack surface through preventative measures; (ii) employing intelligent detection controls at data entry points; and (iii) employing technologies that automatically remedy certain dangerous situations.

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

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. 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 a dual authentication 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 systems from gaining access to systems used to process Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer 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 Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. 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 its 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 background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Google 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), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 3: Specific Privacy Laws

The terms in each subsection of this Appendix 3 apply only where the corresponding law applies to the processing of Customer Personal Data.

European Data Protection Law

1. Additional Definitions.

- "*Adequate Country*" means:

  (a) for data processed subject to the EU GDPR: the European Economic Area, or a country or territory recognized as ensuring adequate protection under the EU GDPR;

  (b) for data processed subject to the UK GDPR: the UK, or a country or territory recognized as ensuring adequate protection under the UK GDPR and the Data Protection Act 2018; or

  (c) for data processed subject to the Swiss FADP: Switzerland, or a country or territory that is: (i) included in the list of the states whose legislation ensures adequate protection as published by the Swiss Federal Data Protection and Information Commissioner, if applicable; or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FADP;

  in each case, other than on the basis of an optional data protection framework.

- "*Alternative Transfer Solution*" means a solution, other than SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.

- "*Customer SCCs*" means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor), or the SCCs (Processor-to-Controller), as applicable.

- "*SCCs*" means the Customer SCCs or SCCs (Processor-to-Processor, Google Exporter), as applicable.

- "*SCCs (Controller-to-Processor)*" means the terms at: https://cloud.google.com/terms/sccs/eu-c2p (https://cloud.google.com/terms/sccs/eu-c2p)

- "*SCCs (Processor-to-Controller)*" means the terms at: https://cloud.google.com/terms/sccs/eu-p2c (https://cloud.google.com/terms/sccs/eu-p2c)
- "*SCCs (Processor-to-Processor)*" means the terms at: https://cloud.google.com/terms/sccs/eu-p2p (https://cloud.google.com/terms/sccs/eu-p2p)
- "*SCCs (Processor-to-Processor, Google Exporter)*" means the terms at: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter (https://cloud.google.com/terms/sccs/eu-p2p-google-exporter)

2. Instruction Notifications. Without prejudice to Google's obligations under Section 5.2 (Compliance with Customer's Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will immediately notify Customer if, in Google's opinion:

a. European Law prohibits Google from complying with an Instruction;

b. an Instruction does not comply with European Data Protection Law; or

c. Google is otherwise unable to comply with an Instruction,

in each case unless such notice is prohibited by European Law.

If Customer is a processor, Customer will immediately forward to the relevant controller any notice provided by Google under this section.

3. Customer's Audit Rights. Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) as described in Section 7.5.2(a) (Customer Audit). During such an audit, Google will make available all information necessary to demonstrate compliance with its obligations under this Addendum and contribute to the audit as described in Section 7.5 (Reviews and Audits of Compliance) and this section.

4. Data Transfers.

4.1 *Restricted Transfers*. The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection Law applies to the transfers (as certified by Customer under Section 4.2 (Certification by Non-EMEA

Customers) of these European Data Protection Law terms, if its billing address is outside EMEA) ("*Restricted Transfers*"), then:

a. if Google has adopted an Alternative Transfer Solution for any Restricted Transfers, Google will inform Customer of the relevant solution and ensure that such Restricted Transfers are made in accordance with it; or

b. if Google has not adopted an Alternative Transfer Solution for any Restricted Transfers, or informs Customer that Google is no longer adopting, an Alternative Transfer Solution for any Restricted Transfers (without adopting a replacement Alternative Transfer Solution):

i. if Google's address is in an Adequate Country:

A. the SCCs (Processor-to-Processor, Google Exporter) will apply with respect to such Restricted Transfers from Google to Subprocessors; and

B. in addition, if Customer's billing address is not in an Adequate Country, the SCCs (Processor-to Controller) will apply (regardless of whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer; or

ii. if Google's address is not in an Adequate Country, the SCCs (Controller-to-Processor) or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer.

4.2 *Certification by Non-EMEA Customers*. If Customer's billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, then unless Appendix 4 (Specific Products) of this Addendum indicates otherwise, Customer will certify as such and identify its competent Supervisory Authority via the Admin Console for the applicable Services.

4.3 *Information about Restricted Transfers*. Google will provide Customer with information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures:

a. as described in Section 7.5.1 (Reviews of Security Documentation);

b. in any additional locations described in Appendix 4 (Specific Products); and

c. in relation to Google's adoption of an Alternative Transfer Solution, at https://cloud.google.com/terms/alternative-transfer-solution (https://cloud.google.com/terms/alternative-transfer-solution).

4.4 *SCC Audits*. If Customer SCCs apply as described in Section 4.1 (Restricted Transfers) of these European Data Protection Law terms, Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

4.5 *SCC Notices*. Customer will forward to the relevant controller promptly and without undue delay any notice that refers to any SCCs.

4.6 *Termination Due to Data Transfer Risk*. If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Google.

4.7 *No Modification of SCCs*. Nothing in the Agreement (including this Addendum) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

4.8 *Precedence of SCCs*. To the extent of any conflict or inconsistency between any Customer SCCs (which are incorporated by reference into this Addendum) and the remainder of the Agreement (including this Addendum), the Customer SCCs will prevail.

5. Requirements for Subprocessor Engagement. European Data Protection Law requires Google to ensure via a written contract that the data protection obligations described in this Addendum, as referred to in Article 28(3) of the GDPR, if applicable, are imposed on any Subprocessor engaged by Google.

CCPA

1. Additional Definitions.

- "*CCPA*" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

- "*Customer Personal Data*" includes "personal information".
- The terms "business", "business purpose", "consumer", "personal information", "processing", "sale", "sell", "service provider", and "share" have the meanings given in the CCPA.

2. Prohibitions. Without prejudice to Google's obligations under Section 5.2 (Compliance with Customer's Instructions), with respect to the processing of Customer Personal Data in accordance with the CCPA, Google will not, unless otherwise permitted under the CCPA:

a. sell or share Customer Personal Data;

b. retain, use or disclose Customer Personal Data:

i. other than for a business purpose under the CCPA on behalf of Customer and for the specific purpose of performing the Services and TSS; or

ii. outside of the direct business relationship between Google and Customer; or

c. combine or update Customer Personal Data with personal information that Google receives from or on behalf of a third party or collects from its own interactions with the consumer.

3. Compliance. Without prejudice to Google's obligations under Section 5.2 (Compliance with Customer's Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will notify Customer if, in Google's opinion, Google is unable to meet its obligations under the CCPA, unless such notice is prohibited by applicable law.

4. Customer Intervention. If Google notifies Customer of any unauthorized use of Customer Personal Data, including under Section 3 (Compliance) of this subsection or Section 7.2.1 (Incident Notification), Customer may take reasonable and appropriate steps to stop or remediate such unauthorized use by:

a. taking any measures recommended by Google pursuant to Section 7.2.2 (Details of Data Incident), if applicable; or

b. exercising its rights under Section 7.5.2(a) (Customer Audit) or 9.1 (Access; Rectification; Restricted Processing; Portability).

Turkey

1. Data Transfers.

1.1 If Customer's billing address is in Turkey and Customer accepts any additional terms made available separately by Google in relation to transfers of Customer Personal Data under the Turkish Law on the Protection of Personal Data No. 6698 dated April 7, 2016, those terms will supplement this Addendum.

1.2 If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Google.

Israel

1. Additional Definition.

- "*Israeli Privacy Protection Law*" means the Israeli Privacy Protection Law, 1981 and any regulations promulgated thereunder.

2. Equivalent Terms. Any terms equivalent to "controller", "personal data", "processing", and "processor", as used in this Addendum, have the meanings given in the Israeli Privacy Protection Law.

3. Customer's Audit Rights. Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) as described in Section 7.5.2(a) (Customer Audit).

Appendix 4: Specific Products

The terms in each subsection of this Appendix 4 apply solely with respect to the processing of Customer Data by the corresponding Service(s).

Google Cloud Platform

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's Google Cloud Platform account.
- "*Customer Data*", if not defined in the Agreement, means data provided to Google by Customer or End Users through Google Cloud Platform under the Account, and data

that Customer or End Users derive from that data through their use of Google Cloud Platform.

- "*Google Cloud Platform*" means the Google Cloud Platform services described at https://cloud.google.com/terms/services (https://cloud.google.com/terms/services), excluding any Third-Party Offerings.
- "*Third-Party Offerings*", if not defined in the Agreement, means (a) third-party services, software, products, and other offerings that are not incorporated into Google Cloud Platform or Software, (b) offerings identified in the "Third-Party Terms" section of the Service Specific Terms of the Agreement, and (c) third-party operating systems.

2. Compliance Certifications. The Compliance Certifications for Google Cloud Platform Audited Services will also include certificates for ISO 27017 and ISO 27018 and a PCI DSS Attestation of Compliance.

3. Data Center Locations. The locations of Google Cloud Platform data centers are described at https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/).

4. Information about Subprocessors. Names, locations, and activities of Google Cloud Platform Subprocessors are described at https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/third-party-suppliers).

5. Cloud Data Protection Team. The Data Protection Team for Google Cloud Platform can be contacted at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo).

6. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures is available at cloud.google.com/privacy (https://cloud.google.com/privacy)/.

7. Service Specific Terms.

Bare Metal Solution (Google Cloud Platform)

Bare Metal Solution provides non-virtualized access to underlying infrastructure resources and, by design, has certain distinct characteristics.

1. Amendments. This Addendum is amended as follows with respect to Bare Metal Solution:

- The definition of "Google's Third-Party Auditor" is replaced with the following:
    - "*Google's Third-Party Auditor*" means a qualified and independent third-party auditor appointed by Google or a Bare Metal Solution Subprocessor, whose then-current identity Google will disclose to Customer on request.
- The following terms are deleted:
    - From Section 7.1.1 (Google's Security Measures), the phrase "encrypt personal data";
    - From Appendix 2 (Security Measures), the Section 1(a) subsections titled "Server Operating Systems" and "Business Continuity";
    - From Appendix 2, the Section 1(b) subsections titled "External Attack Surface," "Intrusion Detection," and "Encryption Technologies"; and
    - From Appendix 2, the following sentences of Section 3(a):
        - 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.

2. Compliance Certifications and SOC Reports. Google or its Subprocessor will maintain at least the following (or an equivalent or enhanced alternative) for Bare Metal Solution to verify the continued effectiveness of the Security Measures:

a. a certificate for ISO 27001 and a PCI DSS Attestation of Compliance (the "*BMS Compliance Certifications*"); and

b. SOC 1 and SOC 2 reports updated annually based on an audit performed at least once every 12 months (the "*BMS SOC Reports*").

3. Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the BMS Compliance Certifications and BMS SOC Reports available for review by Customer and, if Customer is a processor, allow Customer to request access for the relevant controller to the BMS SOC Reports in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

4. Customer Obligations. Without limiting Google's express obligations related to Bare Metal Solution, Customer will take reasonable steps to protect and maintain the security of

Customer Data and any other content stored on or processed through Bare Metal Solution.

5. Disclaimer. Notwithstanding anything to the contrary in the Agreement (including this Addendum), Google is not responsible for any of the following in relation to Bare Metal Solution:

a. non-physical security, such as access controls, encryption, firewalls, antivirus protection, threat detection, and security scanning;

b. logging and monitoring;

c. non-hardware maintenance or support;

d. data backup, including any redundancy or high-availability configuration; or

e. business continuity and disaster recovery policies or procedures.

Customer is solely responsible for securing (other than physical security of Bare Metal Solution servers), logging and monitoring, maintaining and supporting, and backing up any Operating Systems, Customer Data, software, and applications Customer uses with, uploads to, or hosts on Bare Metal Solution.

Google Distributed Cloud Edge (Google Cloud Platform)

Google Distributed Cloud Edge ("*GDCE*") is not deployed at a Google data center and, by design, has certain distinct characteristics.

1. Amendments. This Addendum is amended as follows with respect to GDCE:

- References to "Google's systems" are replaced with "the Equipment."
- Section 6.2 (Return or Deletion When Term Ends) is replaced with the following:
    - 6.2 *Return or Deletion at the end of the Term*. Customer instructs Google to delete all remaining Customer Data (including existing copies) from the Equipment at the end of the Term in accordance with applicable law. If Customer wishes to retain any Customer Data after the end of the Term, it may export or make copies of such data prior to the end of the Term. Google will comply with the Instruction in this Section 6.2 as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

- The following words are added to the end of Section 10.1 (Data Storage and Processing Facilities): "or where the Customer Location is located."
- Section 1 (Data Center and Network Security) of Appendix 2 (Security Measures) is replaced with the following:
    - **1. Local Machines and Network Security**

      Local Machines. Customer Data is solely stored on the Equipment to be deployed in a Customer Location.

      Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Google employs a code review process to increase the security of the code used to provide GDCE and enhance the security products in GDCE production environments.

      Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available and allows for encryption of data in transit. 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. Google also makes encryption of data at rest available, using at least AES128 or similar. GDCE has a CMEK integration; more information can be found at https://cloud.google.com/kms/docs/cmek (https://cloud.google.com/kms/docs/cmek).

      Connection to Cloud VPN. Google allows Customer to enable and configure a strong, encrypted interconnection between the Equipment and Customer's Virtual Private Cloud using Cloud VPN through an IPSEC VPN connection.

      Bound Storage. Customer's data storage is bound to the server. Should a disk be stolen or copied at rest, the contents of such disk will be unrecoverable outside of the server.
- Sections 2 (Access and Site Controls) and 3 (Data) of Appendix 2 (Security Measures) are deleted.

2. Inapplicable Provisions. Any Google obligations in the Agreement (including this Addendum) or statements in associated security documentation (including whitepapers) that depend on Google's operation of a Google data center do not apply to GDCE.

Google-Managed Multi-Cloud (Google Cloud Platform)

Google-Managed Multi-Cloud Services involve third-party infrastructure and, by design, have certain distinct characteristics.

1. Additional Definition.

- "*Google-Managed MCS Data Processing Amendment*" means the terms at https://cloud.google.com/terms/mcs-data-processing-terms (https://cloud.google.com/terms/mcs-data-processing-terms).

2. Multi-Cloud Data Processing Terms. The Google-Managed MCS Data Processing Amendment supplements and amends this Addendum with respect to Google-Managed Multi-Cloud Services for Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google may not have access to Customer's VMware environment or be able to encrypt personal data in Customer's VMware environment.

NetApp Volumes (Google Cloud Platform)

1. Amendments. This Addendum is amended as follows with respect to NetApp Volumes:

- The definition of "Google's Third-Party Auditor" is replaced with the following:
    - "*Google's Third Party Auditor*" means a qualified and independent third party auditor appointed by Google or a NetApp Volumes Subprocessor, whose then-current identity Google will disclose to Customer on request.
- Section 3(a) (Data Storage, Isolation and Logging) of Appendix 2 (Security Measures) is replaced with the following:
    - (a) *Data Storage, Isolation and Logging*. Google stores data in a multi-tenant environment on servers owned by NetApp, Inc. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. 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 its End Users for specific purposes. Customer may

choose to use logging functionality that Google makes available via the Services.

2. Compliance Certifications and SOC Reports. Google or its Subprocessor will obtain at least the following (or an equivalent or enhanced alternative) for NetApp Volumes:

a. a certificate for ISO 27001 and a PCI DSS Attestation of Compliance (the "*NetApp Compliance Certifications*"); and

b. SOC 1 and SOC 2 Reports updated annually based on an audit performed at least once every 12 months (the "*NetApp SOC Reports*").

3. Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make any NetApp Compliance Certifications and NetApp SOC Reports available for review by Customer and, if Customer is a processor, allow Customer to request access for the relevant controller to the NetApp SOC Reports in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

Google Workspace and Cloud Identity

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's Google Workspace or Cloud Identity account.
- "*Cloud Identity*" when purchased under a standalone Agreement and not as part of Google Cloud Platform or Google Workspace, means the Cloud Identity Services described at https://cloud.google.com/terms/identity/user-features (https://cloud.google.com/terms/identity/user-features).
- "*Customer Data*", if not defined in the Agreement, means data submitted, stored, sent or received by or on behalf of Customer or its End Users via Google Workspace or Cloud Identity under the Account.
- "*Google Workspace*" means the Google Workspace or Google Workspace for Education services described at https://workspace.google.com/terms/user_features.html (https://workspace.google.com/terms/user_features.html), as applicable.

2. Additional Products. If Google at its option makes Additional Products available to Customer for use with Google Workspace or Cloud Identity in accordance with applicable

Additional Product Terms:

a. Customer may enable or disable Additional Products via the Admin Console and will not need to use Additional Products in order to use Google Workspace or Cloud Identity; and

b. if Customer opts to install any Additional Products or to use them with Google Workspace or Cloud Identity, the Additional Products may access Customer Data as required to interoperate with Google Workspace or Cloud Identity, as applicable.

For clarity, this Addendum 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.

3. Compliance Certifications. The Compliance Certifications for Google Workspace and Cloud Identity Audited Services will also include certificates for ISO 27017 and ISO 27018.

4. Data Center Locations. The locations of Google Workspace and Cloud Identity data centers are described at https://www.google.com/about/datacenters/locations/ (https://www.google.com/about/datacenters/locations/).

5. Information about Subprocessors. Names, locations, and activities of Google Workspace and Cloud Identity Subprocessors are described at https://workspace.google.com/intl/en/terms/subprocessors.html (https://workspace.google.com/intl/en/terms/subprocessors.html).

6. Cloud Data Protection Team. The Data Protection Team for Google Workspace and Cloud Identity (while Administrators are signed in to their Admin Account) can be contacted at https://support.google.com/a/contact/googlecloud_dpr (https://support.google.com/a/contact/googlecloud_dpr).

7. Additional Security Measures. For Google Workspace and Cloud Identity:

a. Google logically separates each End User's data from the data of other End Users; and

b. 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).

8. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures is

available at cloud.google.com/privacy (https://cloud.google.com/privacy)/.

9. Service Data Addendum. If Google makes an optional Service Data Addendum available for acceptance by Customer in relation to this Addendum, availability of that optional addendum will constitute a "DPA Update" if such term is defined in any Service Data Addendum previously entered into by Customer.

10. Service Specific Terms.

AppSheet (Google Workspace)

1. Amendments. This Addendum is amended as follows with respect to AppSheet:

- The paragraph titled "Server Operating Systems" in Section 1(a) of Appendix 2 (Security Measures) is replaced with the following:
    - *Server Operating Systems*. Google servers use a Linux based implementation customized for the application environment.

2. Additional Data Center Locations. Additional data center locations for AppSheet are described at https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/).

Looker (original)

1. Additional Definitions.

- "*Admin Console*" means any admin console applicable to each Instance.
- "*Google-Managed MCS Data Processing Amendment*" means, if applicable, the terms at https://cloud.google.com/terms/mcs-data-processing-terms (https://cloud.google.com/terms/mcs-data-processing-terms).
- "*Google-Managed Multi-Cloud Services*" means, if applicable, specified Google services, products and features that are hosted on the infrastructure of a third party cloud provider.
- "*Looker (original)*" means an integrated platform (including cloud-based infrastructure, if applicable, and software components including any associated APIs) that enables businesses to analyze data and define business metrics across multiple

data sources made available by Google to Customer under the Agreement. Looker (original) excludes Third-Party Offerings.

- "*Multi-Cloud Service Third-P*arty *Provider*" has the meaning given in the Google-Managed MCS Data Processing Amendment.

- "*Order Form*" has the meaning given in the Agreement, unless Customer has purchased via a reseller or online marketplace or is using Looker only for trial or evaluation purposes under a trial or evaluation agreement, in which case Order Form may mean another written form (email or other electronic means permitted) as authorized by Google.

2. Amendments. This Addendum is amended as follows with respect to Looker (original):

- The definition of "Notification Email Address" is replaced with the following:

  - "Notification Email Address" means the email address(es) designated by Customer in the Order Form or via Looker (as applicable) to receive certain notifications from Google.

- The definitions of "SCCs (Controller-to-Processor)", "SCCs (Processor-to-Controller)", "SCCs (Processor-to-Processor)" and "SCCs (Processor-to-Processor, Google Exporter)" in Appendix 3 (Specific Privacy Laws) are replaced with the following:

  - "*SCCs (Controller-to-Processor)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-c2p (https://cloud.google.com/terms/looker/legal/sccs/eu-c2p);

  - "*SCCs (Processor-to-Controller)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-p2c (https://cloud.google.com/terms/looker/legal/sccs/eu-p2c);

  - "*SCCs (Processor-to-Processor)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p (https://cloud.google.com/terms/looker/legal/sccs/eu-p2p); and

  - "*SCCs (Processor-to-Processor, Google Exporter)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group (https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group).

- The following words are added to the end of Section 10.1 (Data Storage and Processing Facilities): "or where any Multi-Cloud Service Third-Party Providers maintain facilities."

3. Additional Customer Security Responsibilities. Customer is responsible for the security of Customer's environment, databases, and configuration for Looker (original) excluding systems managed and controlled by Google.

4. Compliance Certifications and SOC Reports. The Compliance Certifications and SOC Reports for Looker (original) Audited Services may vary according to the hosting environment in which the relevant Services are used. Google will provide details of the Compliance Certifications and SOC Reports available for specific hosting environments on request.

5. Data Center Locations. The locations of Looker (original) data centers will be described on the applicable Order Form or otherwise identified by Google.

6. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for Looker (original).

7. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures for Looker (original) is available at https://docs.looker.com (https://docs.looker.com).

8. Information about Subprocessors. Names, locations and activities of Subprocessors for Looker (original) are described at:

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors (https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors) and

b. https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/subprocessors).

9. Google-Managed Multi-Cloud (Looker (original))

Google-Managed Multi-Cloud Services involve third-party infrastructure and, by design, have certain distinct characteristics.

9.1 *Multi-Cloud Data Processing Terms*. The Google-Managed MCS Data Processing Amendment supplements and amends this Addendum with respect to Google-Managed

Multi-Cloud Services for Looker (original).

10. Cloud Data Protection Team. The Data Protection Team for Looker (original) can be contacted at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo).

11. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

12. Additional Application Security Measures. Google will implement and maintain the additional Security Measures described below for Looker (original):

a. Google follows at least industry standard practices for security architecture. Proxy servers used for Google's applications help secure access to Looker by providing a single point to filter attacks through IP denylisting and connection rate limiting.

b. Customer administrators control access to applications by Google personnel to provide technical support requested by Customer or End Users.

SecOps Services

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's SecOps Services or Google Cloud Platform account, as applicable.
- "*Customer Data*", if not defined in the Agreement, means data provided to Google by Customer or End Users through SecOps Services under the Account.
- "*SecOps Services*" means Chronicle SIEM, Chronicle SOAR and Mandiant Solutions, each as described at https://cloud.google.com/terms/secops/services (https://cloud.google.com/terms/secops/services), excluding any Third-Party Offerings. For the avoidance of doubt, SecOps Services exclude Mandiant Managed Services and Mandiant Consulting Services.
- "*Third-Party Offerings*", if not defined in the Agreement, means (a) third-party services, software, products, and other offerings that are not incorporated into SecOps Services or Software, and (b) third-party operating systems.

2. Amendments. This Addendum is amended as follows with respect to SecOps Services:

- The definition of "Additional Security Controls" is replaced with the following:
  - *"Additional Security Controls"* means security resources, features, functionality and/or controls (if any) that Customer may use at its option and/or as it determines, including (if any) encryption, logging and monitoring, identity and access management, and security scanning.
- The definition of "Audited Services" is replaced with the following:
  - "*Audited Services*" means the then-current SecOps Services indicated as being in-scope for the relevant certification or report at https://cloud.google.com/security/compliance/secops/services-in-scope (https://cloud.google.com/security/compliance/secops/services-in-scope). Google may not remove any SecOps Services from this URL unless they have been discontinued in accordance with the applicable Agreement.
- The definitions of "SCCs (Controller-to-Processor)", "SCCs (Processor-to-Controller)", "SCCs (Processor-to-Processor)" and "SCCs (Processor-to-Processor, Google Exporter)" in Appendix 3 (Specific Privacy Laws) are replaced with the following:
  - "SCCs (Controller-to-Processor)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-c2p (https://cloud.google.com/terms/secops/sccs/eu-c2p)
  - "SCCs (Processor-to-Controller)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-p2c (https://cloud.google.com/terms/secops/sccs/eu-p2c).
  - "SCCs (Processor-to-Processor)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-p2p (https://cloud.google.com/terms/secops/sccs/eu-p2p)
  - "SCCs (Processor-to-Processor, Google Exporter)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter (https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter)
- Section 7.4 (Compliance Certifications and SOC Reports) of the Addendum is modified to read as follows:

- 7.4 *Compliance Certifications and SOC Reports*. Google will maintain at least the certifications and reports as identified at https://cloud.google.com/security/compliance/secops/services-in-scope (https://cloud.google.com/security/compliance/secops/services-in-scope) for the Audited Services to verify the continued effectiveness of the Security Measures (the "Compliance Certifications" and "SOC Reports").
  Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

3. Data Center Locations. The locations of SecOps Services data centers are described at https://cloud.google.com/terms/secops/data-residency (https://cloud.google.com/terms/secops/data-residency).

4. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for SecOps Services.

5. Information about Subprocessors. Names, locations, and activities of Subprocessors for SecOps Services are described at https://cloud.google.com/terms/secops/subprocessors (https://cloud.google.com/terms/secops/subprocessors).

6. Cloud Data Protection Team. The Data Protection Team for SecOps Services can be contacted at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo) (and/or via such other means as Google may provide from time to time).

7. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

Previous versions of Data Processing and Security Terms:

June 30, 2022 (/terms/data-processing-addendum/index-20220630) *September 24, 2021* (/terms/data-processing-terms/index-20210924) *August 19, 2020*

(/terms/data-processing-terms/index-20200819) *August 10, 2020*
(https://cloud.google.com/terms/data-processing-terms-20200810) *July 17, 2020*
(https://cloud.google.com/terms/data-processing-terms-20200717) *October 11, 2019*
(https://cloud.google.com/terms/data-processing-terms-20191011) *October 1, 2019*
(https://cloud.google.com/terms/data-processing-terms-20191001)
(https://cloud.google.com/terms/data-processing-terms-20180525) *May 25, 2018*
(https://cloud.google.com/terms/data-processing-terms-20180525) *March 13, 2018*
(https://cloud.google.com/terms/data-processing-terms-20180313) *November 9, 2017*
(https://cloud.google.com/terms/data-processing-terms-20171109) *October 11, 2017*
(https://cloud.google.com/terms/data-processing-terms-20171011) *February 7, 2017*
(https://cloud.google.com/terms/data-processing-terms-20170207) *October 6, 2016*
(https://cloud.google.com/terms/data-processing-terms-20161006)

Previous versions of Data Processing Amendment:

July 7, 2022 (https://workspace.google.com/terms/07072022/dpa_terms.html) *September 24, 2021*
(https://workspace.google.com/terms/09242021/dpa_terms.html) *May 27, 2021*
(https://workspace.google.com/terms/05272021/dpa_terms.html) *October 29, 2019*
(https://workspace.google.com/terms/10292019/dpa_terms.html) *May 25, 2018*
(https://workspace.google.com/terms/05252018/dpa_terms.html) *April 25, 2018*
(https://workspace.google.com/terms/04252018/dpa_terms.html) *July 11, 2017*
(https://workspace.google.com/terms/07112017/dpa_terms.html) *November 28, 2016*
(https://workspace.google.com/terms/11282016/dpa_terms.html) *January 7, 2016*
(https://workspace.google.com/terms/01072016/dpa_terms.html) *April 24, 2015*
(https://workspace.google.com/terms/04242015/dpa_terms.html) *April 1, 2014*
(https://workspace.google.com/terms/04012014/dpa_terms.html) *November 14, 2012*
(https://workspace.google.com/terms/11142012/dpa_terms.html)

Previous versions of Data Processing Addendum for Looker (original) Services (Customers):

(https://cloud.google.com/terms/looker/dpst/index-20230214)*February 14, 2023*
(https://cloud.google.com/terms/looker/dpst/index-20230214)*January 4, 2023*
(https://cloud.google.com/terms/looker/dpst/index-20230104)*September 20, 2022*
(https://cloud.google.com/terms/looker/dpst/dpst-20220920)*June 30, 2022*
(https://cloud.google.com/terms/looker/dpst/dpst-20220630)*March 16, 2022*
(https://cloud.google.com/terms/looker/dpst/dpst-20220316)*September 24, 2021*
(https://cloud.google.com/terms/looker/dpst/dpst-20210924)*April 1, 2021*
(https://cloud.google.com/terms/looker/dpst/dpst-20210401)*January 15, 2021*
(https://cloud.google.com/terms/looker/dpst/dpst-20210115)*December 17, 2020*

(https://cloud.google.com/terms/looker/dpst/dpst-20201217)*August 28, 2020*
(https://cloud.google.com/terms/looker/dpst/dpst-20200828)*June 1, 2020*
(https://cloud.google.com/terms/looker/dpst/dpst-20200601)*March 9, 2020*
(https://cloud.google.com/terms/looker/dpst/dpst-20200309)
(https://cloud.google.com/terms/looker/dpst/index-20230214)

Previous versions of SecOps Services DPST (Customers):

February 6, 2023 (/terms/secops/data-processing-terms/index-20230206) November 28, 2022 (/terms/secops/data-processing-terms/index-20221128) September 27, 2021 (/terms/secops/data-processing-terms/index-20210927) October 1, 2020 (/terms/secops/data-processing-terms/index-20201001)

PREVIOUS VERSIONS *(Last modified November 8, 2023)*

August 15, 2023 (/terms/data-processing-addendum/index-20230815)

September 20, 2022 (/terms/data-processing-addendum/index-20220920)