Partner Information Protection Addendum

Version 9

1. General.

(a) Agreement. This Partner Information Protection Addendum (the "**PIPA**") forms part the agreement, end user license agreement, statement of work or related orders, or other agreement(s) between You and Google (collectively the "**Agreement**") and incorporates the mandatory terms in the PIPA and the Controller-Controller SCCs (as defined below) to the extent applicable.

(b) Order of Precedence. To the extent the PIPA conflicts with the Agreement, the PIPA will govern.

(c) Interpretation. The Agreement's defined terms apply unless the PIPA expressly states otherwise. Capitalized terms used but not defined will have the meanings given to them in the Agreement.

2. Defined Terms.

In this PIPA:

(a) "**Alternative Transfer Solution**" means a mechanism other than the Applicable Standard Contract Clauses that enables the lawful transfer of Personal Information from the EEA, UK, or Switzerland to a third country in accordance with Applicable Data Protection Laws, including as applicable, the EU-U.S., Swiss-U.S., or UK-U.S. Privacy Shield self-certification programs or the EU-U.S. Data Privacy Framework, each to the extent approved and operated by the U.S. Department of Commerce (the "**Privacy Shield**"), or another valid certification program in force in accordance with Applicable Data Protection Laws.

(b) "**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with, a party.

(c) "**Applicable Data Protection Laws**" means privacy, data security, and data protection laws, directives, and regulations in any jurisdiction applicable to the Personal Information Processed for the Services including the GDPR, LGPD, and U.S. State Data Protection Laws.

(d) "**Applicable Standards**" mean government standards, industry standards, codes of practice, guidance from Regulators, and best practices applicable to the parties' Processing of Personal Information for the Services, including Alternative Transfer Solutions and the Payment Card Industry Data Security Standards ("**PCI DSS**").

(e) "**Controller-Controller SCCs**" means the European Commission's standard contractual clauses which are standard data protection clauses for the transfer of personal data to Data Controllers established in third countries that do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and set forth at https://business.safety.google/gdprcontrollerterms/sccs/eu-c2c

(f) "**Data Controller**" means an entity that determines the purposes and means of Processing Personal Information. Data Controller also means "controller" as defined by Applicable Data Protection Laws, and "business" as defined in the CCPA.

(g) "**Deidentified Data**" means "de-identified data" or "deidentified data" as defined by U.S. State Data Protection Laws.

(h) "**Disclosing Controller**" means You or the Google Controller that transfers Personal Information to the Google Controller or You under this PIPA as applicable. For purposes of the Controller-Controller SCCs, the Disclosing Controller means the data exporter.

(i) "**End Controller**" means, for each party, the ultimate Data Controller of Personal Information.

(j) "**GDPR**" means (i) the European Union General Data Protection Regulation (EU) 2016/679 (the "**EU GDPR**") on data protection and privacy for all individuals within the European Union ("**EU**") and the European Economic Area ("**EEA**"); (ii) the EU GDPR as incorporated into United Kingdom ("**UK**") law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**"); and (iii) the Federal Data Protection Act of 19 June 1992 (Switzerland) (each as amended, superseded, or replaced).

(k) "**Google**" means the Google Entity that is party to the Agreement.

(l) "**Google End Controller**" means the End Controllers of Personal Information Processed by Google in accordance with Google's applicable privacy policy at http://policies.google.com/privacy or as otherwise notified to You.

(m) "**Google Entity**" means Google LLC , Google Ireland Limited, or another affiliate of Google LLC.

(n) "**includes**" or "**including**" means "including but not limited to."

(o) "**individual**" or "**individuals**" mean natural persons who can be readily identified, directly or indirectly, or data subjects as defined by Applicable Data Protection Laws.

(p) "**LGPD**" means Brazilian Law no. 13,709 for the protection of personal data.

(q) "**Personal Information**" means any information Processed in connection with the Agreement that is (i) about an individual; or (ii) not specifically about an individual but, when combined with other information, may identify an individual. Personal Information includes names, email addresses, postal addresses, telephone numbers, government identification numbers, financial account numbers, payment card information, credit report information, biometric information, online identifiers (including IP addresses and cookie identifiers), network and hardware identifiers, and geolocation information, and any information that constitutes "**personal data**" or "**personal information**" within the meaning of Applicable Data Protection Laws.

(r) "**Process**" or "**Processing**" means to access, handle, create, collect, acquire, receive, record, combine, consult, use, process, alter, store, retain, maintain, retrieve, disclose, or dispose of. Process also includes "processing" within the meaning of Applicable Data Protection Laws.

(s) "**reasonable**" means reasonable and appropriate to (i) the size, scope, and complexity of Your business; (ii) the nature of Personal Information being Processed; and (iii) the need for privacy, confidentiality, and security of Personal Information.

(t) "**Receiving Controller**" means You or the Google Controller that receives Personal Information from the Google Controller or You under this PIPA as applicable. For purposes of the Controller-Controller SCCs, the data importer means the Receiving Controller.

(u) "**Regulator**" or "**Regulatory**" means an entity with supervisory or regulatory authority over Google under Applicable Data Protection Laws.

(v) "**Services**" means any goods, services, operations, or activities for which the parties Process Personal Information under the Agreement.

(w) "**Third-Party Provider**" means an agent or other entity that a party to this Agreement authorizes to act on its behalf in connection with the Services. "Third Party Provider" includes "processor" within the meaning of the Controller-Controller SCCs.

(x) "**U.S. State Data Protection Laws**" means privacy, data security, and data protection laws and regulations within the United States applicable to the personal information processed by a party under the Agreement and includes (i) Virginia's Consumer Data Protection Act, Va. Code Ann. § 59.1-571 et seq.; (ii) the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq.; (iii) Connecticut's Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015; (iv) the Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.; (v) 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 (the "**CCPA**"); and (vi) data privacy or data protection laws modeled on any of the foregoing, each as may be in effect and applicable to the parties' Processing of Personal Information.

(y) "**You**" or "**Your**" means the party (including any personnel, contractor, or agent acting on behalf of that party) that performs Services for Google or its affiliates under the Agreement.

3. Data Controllers’ Mutual Representations and Warranties.

The parties represent and warrant that each:

(a) is an independent Data Controller with respect to the Personal Information, and

(b) will individually determine the purposes and means of its Processing of Personal Information received from the Disclosing Controller as described in the Agreement.

4. Data Controllers’ Mutual Obligations.

Each party will comply as an independent business with Applicable Data Protection Laws, including to the extent applicable:

(a) Processing Personal Information only where the party maintains a lawful basis of Processing;

(b) providing all required notices or obtaining all required consents from individuals before Processing Personal Information, or disclosing Personal Information to the Receiving Controller;

(c) providing individuals with rights in connection with Personal Information in a timely manner, including the ability of individuals to: (i) access or receive their Personal Information in an agreed upon format; and (ii) correct, amend, or delete Personal Information where it is inaccurate, or has been Processed in violation of Applicable Data Protection Laws;

(d) responding to individual requests or a Regulator concerning the party’s Processing of Personal Information;

(e) maintaining appropriate age verification mechanisms in compliance with Applicable Standards and Applicable Data Protection Laws where a party Processes Personal Information related to individuals under the age of 18; and

(f) Processing Deidentified Data received from the other party in a manner that complies with applicable U.S. State Data Protection Laws.

5. Receiving Controller’s Obligations.

(a) Safeguards. The Receiving Controller will have in place reasonable technical and organizational measures to protect Personal Information against accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure, or access. The Receiving Controller will ensure that such measures provide a level of security reasonable to the risk represented by the Processing and the nature of the data to be protected including:

(i) maintaining reasonable controls to ensure that access to Personal Information will be limited to personnel or Third Party Providers who have a legitimate need to Process Personal Information under the Agreement;

(ii) promptly terminating personnel and Third Party Provider access to Personal Information when such access is no longer required for performance under the Agreement;

(iii) using reasonable and secure data transfer methods to transfer any Personal Information across any network other than an internal company network owned and managed by that party;

(iv) assuming responsibility for any unauthorized access to Personal Information under the Receiving Controller’s custody or control (or Third-Party Provider(s)’ custody or control);

(v) providing reasonable ongoing privacy and information protection training and supervision for all personnel (including Third-Party Providers) who Process Personal Information; and

(vi) maintaining a reasonable incident response program to respond to security incidents, publish a point of contact for security reports on the Receiving Controller’s website, and monitor security reports.

(b) Security Incident Response; Statements. Where required by Applicable Data Protection Laws, the Receiving Controller will promptly inform the Disclosing Controller of a security incident or data protection breach concerning Personal Information. Except as required by law, the Receiving Controller will not make (or permit any Third-Party Provider under its control to make) any statement concerning the security incident that directly or indirectly references the Disclosing Controller unless the Disclosing Controller provides its written authorization.

(c) Third-Party Providers. The Receiving Controller will contractually require each Third-Party Provider that Processes Personal Information to protect the privacy, confidentiality, and security of Personal Information using all reasonable measures as required by this PIPA and Applicable Data Protection Laws. The Receiving Controller will regularly assess its Third-Party Providers’ compliance with these contractual requirements.

(d) Owned or Managed Systems. To the extent the Receiving Controller accesses the Disclosing Controller’s owned or managed networks, systems, or devices (including APIs, corporate email accounts, equipment, or facilities) to Process the Disclosing Controller’s Personal Information, the Receiving Controller will comply with the Disclosing Controller’s written instructions.

(e) Assessments of Compliance with this PIPA. Upon the Disclosing Controller’s written request to assess Receiving Controller’s compliance with the PIPA, the Receiving Controller will, as reasonable and relevant to the Processing, provide certification, audit reports, or other reports regarding the Receiving Controller’s compliance with this PIPA and Applicable Standards as defined by the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), or Statement on Standards for Attestation Engagements (SSAE) and International Standard on Assurance Engagements (ISAE) as published by the American Institute of Certified Public Accountants (AICPA), Payment Card Industry Data Security Standards, and International Auditing and Assurance Standards Board (IAASB), respectively. Examples of acceptable reports include: (1) SOC 1 Type II (based on SSAE 16, 18 or ISAE 3402); (2) SOC 2 Type II (based on SSAE 16, 18 or ISAE 3402); (3) ISO/IEC 27001:2013 certification; and (4) PCI DSS certification.

(f) CCPA Obligations. To the extent Receiving Controller receives Personal Information that is subject to the CCPA from Disclosing Controller through a transfer that qualifies as a "sale" or "sharing," as defined by the CCPA, Receiving Controller will: (i) Process such Personal Information only for the purposes specified in the Agreement; (ii) permit Disclosing Controller, upon reasonable request, to take reasonable and appropriate steps to ensure that Receiving Controller uses the Personal Information in a manner consistent with a business’ obligations under the CCPA by requesting that Receiving Controller attest to its compliance with the CCPA; and (iii) notify Disclosing Controller if it can no longer meet its obligations under the CCPA. If Disclosing Controller reasonably believes that Receiving Controller is engaged in unauthorized processing of the Personal Information, Disclosing Controller will immediately notify Receiving Controller of such belief, and the parties will work together in good faith to remediate the allegedly violative processing activities, if necessary.

6. End Controller.

Without reducing either party’s obligations under the PIPA, each party acknowledges that: (a) the other party’s Affiliates or clients may be End Controller; and (b) the other party may act as a processor on behalf of its End Controller. The Google End Controllers are: (i) for Personal Information subject to the EU GDPR and Processed by Google, Google Ireland Limited and, where the Agreement is with a different Google Affiliate, that Affiliate will be the Google End Controller responsible for Processing Personal Information subject to the EU GDPR in connection with billing for the Services only; and (ii) for Personal Information subject to the UK GDPR and Processed by Google, Google LLC. Each party will ensure that its End Controllers comply with the Controller Terms, including (where applicable) the Controller SCCs.

7. Data Transfers.

Each party may transfer Personal Information if it complies with applicable provisions on the transfer of Personal Information required by Applicable Data Protection Laws.

(a) To the extent a Disclosing Controller transfers Personal Information relating to individuals within the UK, EEA, or Switzerland to a Receiving Controller that is not: (i) subject to the binding obligations of a valid Alternative Transfer Solution; or (ii) located within the EEA or a location that is subject to a valid adequacy decision (as determined by the Applicable Data Protection Laws the parties expressly agree to the Controller-Controller SCCs including the warranties and undertakings contained therein as the “data exporter” and “data importer” as applicable to the transfer of Personal Information contemplated by the parties.

(b) To the extent the Disclosing Controller transfers Personal Information to the Receiving Controller in accordance with an Alternative Transfer Solution, the Receiving Controller will: (i) provide at least the same level of protection for the Personal Information as is required by the Agreement and the applicable Alternative Transfer Solution; (ii) promptly notify the Disclosing Controller in writing if the Receiving Controller determines that it can no longer provide at least the same level of protection for the Personal Information as is required by the Agreement and applicable Alternative Transfer Solution; and (iii) upon making such a determination, cease Processing Personal Information until the Receiving Controller is able to continue providing at least the same level of protection as required by the Agreement and the applicable Alternative Transfer Solution.

(c) Google LLC has certified under the Privacy Shield on behalf of itself and certain wholly-owned US subsidiaries. Google’s certification and status is available at https://www.commerce.gov/page/eu-us-privacy-shield.

(d) Where Google is not the Google Controller, Google will ensure that it is authorized by the Google Controller to (i) enter into the Controller-Controller SCCs on behalf of the Google Controller; and (ii) exercise all rights and obligations on behalf of the Google Controller, each as if it were the Data Controller.

8. Termination.

In addition to the suspension and termination rights in the Agreement, either party may terminate the Agreement or an applicable SOW if it reasonably determines that (a) the other party has failed to cure material noncompliance with the PIPA within a reasonable time; or (b) it needs to do so to comply with Applicable Data Protection Laws.

9. Survival.

This PIPA will survive expiration or termination of the Agreement as long as the parties continue to Process the other party’s Personal Information.

10. Changes to URLs

Google may change any link or URL referenced in this PIPA and the content at any such URL, except that Google may only:

(a) change the Controller-Controller SCCs in accordance with Section 11 (Changes to the PIPA) or to incorporate any new version of the Controller-Controller SCCs that may be adopted under Applicable Data Protection Laws, in each case in a manner that does not affect the validity of the Controller-Controller SCCs; and

(b) make available an Alternative Transfer Solution in accordance with Section 11 (Changes to the PIPA) or to incorporate any new versions of Alternative Transfer Solutions that may be adopted under Applicable Data Protection Laws. For the purposes of this Section 10(b), Google may add a new URL and amend the content of such URL in order to make available such Alternative Transfer Solution.

11. Changes to the PIPA.

Google may change this PIPA if the change:

(a) is permitted by this PIPA, including as described in Section 10(a) (Changes to URLs);

(b) reflects a change in the name or form of a legal entity;

(c) is necessary to comply with an Applicable Data Protection Law, or a binding Regulatory or court order; or

(d) does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, either party’s right to use or otherwise Process the data in scope of the PIPA; and (iii) otherwise have a material adverse impact on the parties’ rights under this PIPA, as reasonably determined by Google.

Partner Information Protection Addendum Version 9

8 December 2022

Previous Versions

- 27 September 2021
- 26 February 2021