Information Protection Addendum

Version 11

Part A: General Information Protection Terms

1. Introduction.

1.1 Status of the Addendum. This Information Protection Addendum (**"IPA"**) forms part of the services agreement(s), statement(s) of work, related order(s), or other commercial terms between You and Google (the "**Agreement**") and incorporates (a) the mandatory terms set out in this Part A (General Information Protection Terms), (b) the Supplemental Terms (as defined below), to the extent applicable, and (c) the Applicable Standard Contractual Clauses (as defined below), to the extent applicable.

1.2 Order of Precedence. To the extent this IPA conflicts with the rest of the Agreement, this IPA will govern.

1.3 Supplemental Terms. The following supplemental terms ("**Supplemental Terms**") apply as set forth below:

(a) Part B (Business Process Outsourcing Requirements) of this IPA will apply to the extent both of the following conditions apply: (i) Your personnel are provisioned with access to Protected Information on Google-owned systems or endpoints and (ii) at least 15 of Your personnel will be providing services to Google from Your work location.

(b) Part C (HIPAA Business Associate Requirements) of this IPA will apply to the extent the Services include access to Personal Information subject to the Health Insurance Portability and Accountability Act of 1996 (**"HIPAA"**).

(c) Supplemental Supplier and Partner Security Standards at https://g.co/partner-security will apply to the extent the Services include software development or web development services.

2. Definitions; Interpretation.

2.1 Definitions. In this IPA:

(a) "**APPI**" means the Japan Act on the Protection of Personal Information, Act No. 57 (including as amended by the 2022 Amended Act on the Protection of Personal Information).

(b) "**Applicable Data Protection Laws**" means all privacy, data security, and data protection laws, directives, regulations, or rules in any jurisdiction applicable to the Personal Information or De-identified Data Processed for the Services, including the APPI, GDPR, LGPD, HIPAA, GLBA, and U.S. State Data Protection Laws.

(c) "**Applicable Standard Contractual Clauses**" means the European Commission's standard contractual clauses, which are standard data protection clauses for the transfer of personal data to third countries that do not ensure an adequate level of data protection, as described in Article 46 of the EU GDPR including the Controller-Processor SCCs or Controller-Controller SCCs.

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

(e) "**Controller-Controller SCCs**" means the terms at https://business.safety.google/gdprcontrollerterms/sccs/eu-c2c.

(f) "**Controller-Processor SCCs**" means the terms at https://business.safety.google/gdprcontrollerterms/sccs/eu-c2p-ipa.

(g) "**Data Controller**" means the legal entity or party to the Agreement that determines the purposes and means of Processing Personal Information. Data Controller also means "controller", "business", or "covered entity" as defined by Applicable Data Protection Laws.

(h) "**Data Processor**" means the legal entity or party to the Agreement that Processes Personal Information on behalf of a Data Controller. Data Processor also means "processor", "contractor", or "service provider" within the meaning of Applicable Data Protection Laws.

(i) "**Data Transfer Solution**" means a solution that enables the lawful transfer of Personal Information to a third country in accordance with the GDPR or other Applicable Data Protection Laws, including the EU-U.S. Data Privacy Framework, UK Extension to EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework (collectively, the "**Data Privacy Framework**"), or another valid data protection framework recognized as providing adequate protection under GDPR or other Applicable Data Protection Laws.

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

(k) "**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**"), including all applicable EU Member State and EEA country laws implementing the EU GDPR; (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).

(l) "**GLBA**" means the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, 15 U.S.C. §§ 6801-08, 6821-27 (1999).

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

(n) "**Google Controller**" means the Google Entity that Processes Personal Information as a Data Controller in accordance with Google's applicable privacy policy at https://policies.google.com/privacy, or as notified to You.

(o) "**Google Entity**" means Google LLC (formerly known as Google Inc.), Google Ireland Limited, or another affiliate of Google LLC.

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

(q) "**individual**" or "**individuals**" mean natural persons who can be any natural person to whom any Personal Information relates, including "data subjects" and "consumers", as defined by Applicable Data Protection Laws.

(r) "**LGPD**" means Brazilian Law 13,709 for the protection of personal data.

(s) "**MVSP**" means the business controls, application design controls, application implementation controls, and operational controls as set forth in the most recent version of the Minimum Viable Secure Product (the "**MVSP**") available at (https://mvsp.dev/mvsp.en/index.html).

(t) "**Personal Information**" means any information about an individual or information that is not specifically about an individual but, when combined with other information, may identify an individual or any other information that constitutes "personal data" or "personal information" within the meaning of Applicable Data Protection Laws and, without limitation, 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 that is Processed in connection with the Services.

(u) "**Process**" or "**Processing**" will have the meaning provided under Applicable Data Protection Laws relevant to Personal Information, and where such definition is not specified, will have the meaning provided under the EU GDPR.

(v) "**Protected Information**" means Personal Information, De-identified Data, or any confidential information (as marked by the parties or defined in the Agreement as Confidential Information) that You or a Third Party Provider may Process in performing Services. Personal Information and Protected Information does not include the parties' phone numbers, email addresses, or other reasonably limited information used solely to facilitate the parties' communications for administration of the Agreement.

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

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

(y) "**Safeguards**" means the technical, organizational, administrative, and physical controls described in Section 5 (Safeguards), Section 6 (Encryption Requirements), Section 7 (Use of Google Networks, Systems, or Devices), Section 8.3 (Your Continuous Self-Assessment), Section 9.1 (Security Incident Response Program), and Section 11 (PCI Compliance).

(z) "**Secondary Use**" means any Processing of Personal Information for purposes other than as necessary to fulfill Your business purpose (as defined by Applicable Data Protection Laws) and obligations set forth in the Agreement, including: (i) Processing Personal Information for purposes other than specified in the Services; (ii) Processing Personal Information in combination with any Personal Information that You Process outside of the Services; (iii) Processing Personal Information in any manner that would constitute a sale, targeted advertising, or cross-context behavioral advertising of Personal Information as defined by Applicable Data Protection Laws, or (iv) Processing Personal Information outside of the direct business relationship between You and Google.

(aa) "**Security Incident**" means actual or reasonable degree of certainty of unauthorized use, destruction, loss, control, alteration, acquisition, exfiltration, theft, retention, disclosure of, or access to, Protected Information for which You are responsible. Security Incidents do not include unsuccessful access attempts or attacks that do not compromise the confidentiality, integrity, or availability of Protected Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(bb) "**Services**" means any goods or services that You or a Third Party Provider provide(s) to or for Google under the Agreement.

(cc) "**Supplemental Supplier and Partner Security Standards**" means the obligations, standards, and requirements set forth at http://g.co/partner-security.

(dd) "**Third Party Provider**" means any parent company, subsidiary, agent, contractor, processor, service provider, sub-contractor, sub-processor, or other third party You authorize to act on Your behalf in connection with the Processing of Personal Information intended for the Services. "Third Party Provider" includes "subprocessor" within the meaning of the Applicable Standard Contractual Clauses.

(ee) "**U.S. State Data Protection Laws**" means all privacy, data security and data protection laws, regulations or rules in the United States applicable to the Personal Information Processed for the Services, including without limitation the laws listed at business.safety.google/usdataprotectionlaws.

(ff) "**You**" or "**Your**" means the party (including any personnel, contractor, or agent acting on behalf of such party) that performs Services for Google or its affiliates under the Agreement. References to "You" and "Your" herein include any Third Party Providers.

2.2 Interpretation and Defined Terms. The Agreement's defined terms apply to this IPA unless this IPA expressly states otherwise. Capitalized terms used but not defined will have the meanings given to them in the Agreement.

3. Your Data Protection Obligations.

3.1 General Obligations. When You Process Google's Protected Information, You will at all times:

(a) comply with Applicable Data Protection Laws and Applicable Standards;

(b) Except where Section 3.4 (Obligations Where You Process Personal Information as a Data Controller) applies, Process Protected Information only on behalf of Google and in accordance with the limited and specified purposes of Processing, business purpose, and instructions stated in the Agreement, and not for a Secondary Use

(c) assist Google in complying with lawful requests of individuals regarding Your Processing of Personal Information, including all requests made by individuals pursuant to Applicable Data Protection Laws; and

(d) promptly notify Google if You believe (i) compliance with this IPA will interfere with your obligations under Applicable Data Protection Laws; or (ii) You can no longer meet Your obligations under this IPA.

3.2 Data Transfers. The parties will comply with Applicable Data Protection Laws relating to the transfer of Personal Information to third countries:

(a) Google LLC has certified under the Data Privacy Framework on behalf of itself and certain of its wholly-owned U.S. subsidiaries. Google LLC's certification is available at https://www.dataprivacyframework.gov. The Data Privacy Framework will apply to any transfer to a certified Google entity in the U.S. of Personal Information subject to the GDPR.

(b) To the extent either party transfers Personal Information subject to the GDPR, and the party receiving the Personal Information is (i) not located within the EEA, (ii) not located in a country that is subject to a valid adequacy decision (as determined by the Applicable Data Protection Laws), or (iii) not subject to the binding obligations of a valid Data Transfer Solution, the parties expressly agree to transfer the Personal Information in accordance with a Data Transfer Solution, where applicable. Where a Data Transfer Solution does not apply, the parties expressly agree to the Applicable Standard Contractual Clauses including the warranties and undertakings contained therein as the "data exporter" and "data importer" as applicable to the transfer contemplated by the parties.

(c) To the extent the parties agree to transfer Personal Information pursuant to the Applicable Standard Contractual Clauses and You Process Personal Information as a Data Processor, You and Google (on its own behalf or on behalf of the Google Controller) agree to the Controller-Processor SCCs.

(d) To the extent the parties agree to transfer Personal Information pursuant to the Applicable Standard Contractual Clauses and You Process Personal

Information as a Data Controller, You and Google (on its own behalf or on behalf of the Google Controller) agree to the Controller-Controller SCCs.

(e) To the extent either party Processes Personal Information transferred in accordance with a Data Transfer Solution, the party receiving Personal Information will: (i) provide at least the same level of protection for the Personal Information as is required by the Agreement and the applicable Data Transfer Solution; (ii) promptly notify the party disclosing Personal Information in writing if the receiving party 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 Data Transfer Solution; and (iii) upon making such a determination, cease Processing Personal Information until the party receiving Personal Information is able to continue providing at least the same level of protection as required by the Agreement and the applicable Data Transfer Solution.

(f) Where Google is not the Google Controller, Google will ensure that it is authorized by the Google Controller to (i) enter into the Applicable Standard Contractual Clauses 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.

3.3 Your Processing Role. You will Process Personal Information as a Data Processor unless (i) the Agreement expressly authorizes You to Process Personal Information as a Data Controller for a particular Processing activity under the Services; or (ii) Applicable Data Protection Laws strictly require You to Process Personal Information as a Data Controller for a particular Processing activity contemplated by the Services.

3.4 Obligations Where You Process Personal Information as a Data Controller. If permitted by Section 3.3 (Your Processing Role) to Process Personal Information as a Data Controller, You will comply with Applicable Data Protection Laws, including to the extent applicable:

(a) maintaining a lawful basis of Processing Personal Information;

(b) Processing Personal Information consistent with and subject to the limited and specified purposes of Processing described in the Agreement and, where required by Applicable Data Protection Law, consistent with any consent provided by the relevant individuals;

(c) making all required notices, maintaining required opt-out mechanisms, and obtaining all required consents from individuals before Processing Personal Information, including where You disclose Personal Information to Google;

(d) providing individuals with rights required by Applicable Data Protection Laws 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;

(e) responding to individual requests or a Regulator concerning Your Processing of Personal Information;

(f) where permitted to Process Children's Personal Information (as defined in Section 5.5), maintaining appropriate age verification mechanisms capable of enabling Google to comply with Applicable Standards and Applicable Data Protection Laws relating to Children's Personal Information.

4. Third Party Providers.

You may not subcontract the performance of any part of the Services that would cause a Third Party Provider to Process Protected Information without Google's prior written authorization. You will send any requests for Google's consent to the subcontracting of any part of the Services to a Third Party Provider to subprocessor-compliance@google.com or the following external webform available at (https://sites.google.com/corp/view/subprocessor-notifications/home). If and to the extent Google gives such prior authorization, You will:

(a) carry out adequate due diligence of Your Third Party Provider to ensure its capability of providing the level of security and privacy required by the Agreement, including this IPA, and annually review such Third Party Provider to ensure it maintains such capability;

(b) engage Your Third Party Provider pursuant to a written contract that imposes the same restrictions and obligations with respect to the processing of Protected Information that are required of You under this IPA;

(c) retain oversight of and be responsible for Your Third Party Providers' acts and omissions in connection with the Agreement;

(d) on reasonable request, provide Google with information about any authorized Third Party Provider, including a description of contractual terms with such Third Party Provider; and

(e) publish a list of Third Party Providers with access to Protected Information on Your website.

Subject to Applicable Data Protection Laws, Google will take reasonable efforts to maintain Your reasonable confidentiality obligations to Third Party Providers.

5. Safeguards.

At all times that You Process Protected Information, You will maintain the security measures described in the MVSP, as well as controls that meet Applicable Standards, and Applicable Data Protection Laws, including the following:

5.1 Physical Controls. You will maintain physical controls designed to secure relevant facilities, including layered controls covering perimeter and interior barriers, physical access controls, strongly-constructed facilities, suitable locks with key management procedures, access logging, and intruder alarms/alerts and response procedures.

5.2 Technical Controls. To the extent You Process Protected Information on systems not owned and controlled by Google, You will:

(a) establish and enforce access control policies and measures to ensure that only Your personnel who have a legitimate need to Process Protected Information will have such access, including multi-factor authentication;

(b) promptly terminate Your personnels' access to Protected Information when such access is no longer required, and perform regular reviews of access to validate legitimate need to access Protected Information;

(c) maintain reasonable and up-to-date anti-malware, anti-spam, and similar controls on Your networks, systems, and devices;

(d) log the appropriate details of access to Protected Information on Your systems and equipment, including: users logging in and out; reading, writing, or deleting operations on applications and system objectives; or security settings changes (including disabling logging). Logs should include user name, IP address, valid timestamp, action performed, and object of this action and should be retained for no fewer than 90 days;

(e) maintain controls and processes designed to ensure that all operating system and application security patches are installed within the timeframe recommended or required by the issuer of the patch and in a manner consistent with the practices described in the MVSP;

(f) maintain password requirements consistent with the practices described in the MVSP;

(g) implement reasonable user account management procedures to securely create, amend, and delete user accounts on networks, systems, and devices through which You Process Protected Information, including monitoring redundant accounts and ensuring that information owners properly authorize all

user account requests;

(h) back up and secure Protected Information to a different location from where the application is running;

(i) maintain and periodically test disaster recovery plans, including by testing backup restoration; and

(j) publish a point of contact for security reports on Your website and reasonably monitor and respond to security reports.

5.3 Personnel Training and Supervision. You will provide reasonable ongoing privacy and information security training and supervision for Your personnel who Process Protected Information. You will maintain policies and practices restricting access to Protected Information, including having appropriate use guidelines and written confidentiality agreements and performing background checks in accordance with Applicable Data Protection Laws on all individuals who Process Protected Information on Your behalf or who implement, maintain, or administer Your Safeguards. You will ensure that Your personnel are made aware that access to Google internal systems will be monitored, logged, and processed subject to Google's policies relating to data protection.

5.4 Supplemental Supplier and Partner Security Standards. To the extent the Services include software development, application development, or web development services, You will:

(a) comply with the Supplemental Supplier and Partner Security Standards and ensure the Services adheres with the MVSP controls;

(b) maintain current documentation about the Processing of Protected Information, including a list of sensitive data types expected to be Processed and a diagram indicating how Protected Information reaches and is stored on Your systems; and

(c) maintain secure development guidelines and train Your personnel responsible for developing software, applications, or web services to prevent security vulnerabilities, including: authorization bypass, insecure session identifiers, injections, cross-site scripting, cross-site request forgery, and the use of vulnerable libraries.

5.5 Additional Safeguards for Personal Information about Children. To the extent You Process Personal Information relating to individuals under the age of 18 ("**Children**"), You will:

(a) implement measures to safeguard Personal Information relating to Children at the highest reasonable level of protection, including measures reasonably requested by Google. Such measures will take into account the fact that Children require specific protection with regard to their Personal Information and will aim at protecting the best interests of Children;

(b) provide reasonable assistance to Google to allow Google to comply with Applicable Standards relating to Children's Personal Information, and not by act or omission prevent Google's compliance with such Applicable Standards; and

(c) not Process Personal Information relating to Children in ways that have been shown to be detrimental to Children's wellbeing.

Google may suspend the sharing of Children's Personal Information with You if it reasonably determines that You have failed to comply with this Section 5.5, until You remedy such failure.

6. Encryption Requirements.

Using a reasonable encryption standard, You will encrypt Protected Information that is (a) transferred across any external network not solely managed by You; (b) maintained at rest on Your systems; (c) stored on portable devices or portable electronic media (including any backups); or (d) maintained outside of Google's or Your facilities. You will encrypt all Personal Information where required by Applicable Data Protection Laws.

7. Use of Google Networks, Systems, or Devices.

To the extent that You access Google-owned or Google-managed networks, systems, or devices (including Google APIs, corporate email accounts, equipment, or facilities) to Process Protected Information, You will comply with Google's written instructions, system requirements, training requirements, and policies made available to You.

8. Assessments; Audits; Correcting Vulnerabilities.

8.1 Data Protection Assessments. Upon Google's written request, You will promptly and accurately complete Google's assessment of Your compliance with this IPA, Applicable Data Protection Laws, the MVSP, or Applicable Standards. You will provide all reasonably requested information and evidence relating to Your networks, applications, or systems used to Process Protected Information capable of demonstrating that You are complying with this IPA and Applicable Data Protection Laws. You will also permit reasonable access to Your personnel, information, documentation, infrastructure, policies, and application software, to the extent any of the foregoing is involved in Your access to Protected Information and reasonably related to Your obligations under this IPA or Applicable Data Protection Laws.

8.2 Penetration Testing. If You Process Protected Information from Your systems, or Your systems connect to Google's internal systems, then the following will apply:

(a) Google Conducted Penetration Test. Upon reasonable notice, Google (or Google's independent third party assessor that is not Your competitor) may perform annual penetration testing or other periodic security assessments on Your systems used to Process Protected Information. Google reserves the right to perform more frequent testing in connection with material changes to Services, changes to Safeguards required by Applicable Data Protection Laws, or as a result of any material vulnerability or Security Incident notified to Google.

(b) Third Party Conducted Penetration Test. Instead of a Google-conducted penetration test under Section 8.2(a), at Google's sole discretion Google may accept the written results of penetration testing (and the status of Your efforts to remediate findings, if any) performed by Your accredited third party vulnerability tester and at Your own cost following commonly accepted guidelines consistent with Google's then current Testing Guidelines set forth at https://partner-security.withgoogle.com/docs/pentest_guidelines. The penetration testing report must be in English or accompanied by an English translation. Google will treat the information You disclose in connection with this Section 8 as Your Confidential Information.

For the purpose of this Section 8.2, Google will agree to test Your systems in a non-production environment, so long as You provide reasonable evidence to Google's satisfaction that the testing environment is similar to the production environment in functionality.

8.3 Your Continuous Self-Assessment. You will continuously monitor risk to Protected Information and ensure that the Safeguards are properly designed and maintained to protect the confidentiality, integrity, and availability of Protected Information. As part of Your continuous self-assessment program, You will: (a) periodically (but no less than once per year) (i) perform an assessment using the MVSP checklist, and (ii) ensure third party penetration tests consistent with Google's then current Testing Guidelines set forth at https://partner-security.withgoogle.com/docs/pentest_guidelines, and other appropriate vulnerability tests are conducted, and document the effectiveness of Your Safeguards; (b) promptly fix high and critical severity findings; and (c) promptly apply any high or critical severity security patches to Your production servers, endpoints, and endpoint management systems.

8.4 Data Protection Audits.

(a) Audits and Certifications. Upon written request by Google, not more than once per year, Google may conduct an audit of Your architecture, systems, processes, and procedures relevant to the protection of Personal Information at locations where Personal Information is Processed. You will work cooperatively with Google to agree on an audit plan in advance of any audit. If the scope of the audit is addressed in a SSAE 16/SOC1, SOC2, ISO 27001/27701, NIST, PCI DSS, HITRUST, or similar audit report performed by a qualified third party auditor within the prior 12 months, and Your data protection or other relevant officer certifies in writing there are no known material changes in the controls audited, Google may agree to accept those reports in lieu of requesting an audit of the controls covered by the report.

(b) Regulatory Audit. Notwithstanding Section 8.4(a), You will reasonably cooperate and assist Google (i) where a Regulator requires an audit of the data processing facilities from which You process Personal Information in order to ascertain or monitor Google's compliance with Applicable Data Protection Laws; (ii) in the undertaking of a data protection impact assessment or prior consultation with a Regulator; and (iii) by making available information in Your possession that is necessary to demonstrate Your compliance with the IPA.

8.5 Correcting Vulnerabilities. You will apply security patches to all components of the application stack with severity score higher than "low" or "optional" as determined by the issuer of the patch within one month after release. If either party discovers that Your Safeguards contain a vulnerability, You will promptly correct or mitigate at Your own cost (a) any vulnerability within a reasonable period, and (b) any material vulnerability within a period not to exceed 90 days. If You are unable to correct or mitigate the vulnerabilities within the specified time period, You must promptly notify Google and propose reasonable remedies. Compliance with this Section 8.5 will not reduce or suspend Your obligations under Sections 9 (Security Incident Response) and 13 (Records; Destruction; Responding to Individual Requests; Sanitization) or Google's rights under Section 12 (Suspension; Termination).

8.6 Other Confidential Information. Google will take reasonable efforts to protect confidential information that You make available to Google under this Section 8 and respect Your confidentiality obligations to those not subject to the Agreement.

9. Security Incident Response.

9.1 Security Incident Response Program. You will maintain a reasonable Security Incident response program.

9.2 Security Incident Notification.

(a) If You become aware of a Security Incident, You will promptly: (i) stop the unauthorized access; (ii) secure Protected Information; (iii) notify Google (in no event more than 72 hours after discovery of the Security Incident) by sending an email to external-incidents@google.com with the information described in Section 9.2(b) below, even if You have not conclusively established the nature or extent of the Security Incident; and (iv) assist Google in complying with its Security Incident notification or cure obligations under Applicable Data Protection Laws and as otherwise reasonably requested.

(b) You will provide reasonable information about the Security Incident, including: (i) a description of Protected Information subject to the Security Incident (including the categories and number of data records and individuals concerned) and the likely consequences of the Security Incident; (ii) the date and time of the Security Incident; (iii) a description of the circumstances that led to the Security Incident (e.g., loss, theft, copying); (iv) a description of the measures You have taken and propose to take to address the Security Incident; and (v) relevant contact people who will be reasonably available until the parties mutually agree that the Security Incident has been resolved. For Security Incidents involving Personal Information, "reasonably available" means 24 hours per day, 7 days per week.

9.3 Remediation; Investigation. At Your cost, You will take appropriate steps to promptly remediate the root cause(s) of any Security Incident, and will reasonably cooperate with Google with respect to the investigation and remediation of such incident, including providing such assistance as required to enable Google to satisfy its obligation to notify individuals and cure an alleged violation related to a Security Incident. You will promptly provide Google the results of the investigation and any remediation already undertaken. You will not engage in any action or inaction that unreasonably prevents Google from curing an alleged violation of Applicable Data Protection Laws.

9.4 No Unauthorized Statements. Except as required by Applicable Data Protection Laws, You will not make (or permit any third party to make) any statement concerning the Security Incident that directly or indirectly references Google, unless Google provides its explicit written authorization.

10. Legal Process.

If You or anyone to whom You provide access to Protected Information becomes legally compelled by a court or other government authority to disclose Protected Information, then to the extent permitted by law, You will promptly inform Google of any request and reasonably cooperate with Google's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action as Google may deem appropriate. Unless required by Applicable Data Protection Laws, You will not respond to such request, unless Google has authorized You to do so.

11. PCI Compliance.

To the extent You receive, process, transmit, or store any Cardholder Data for or on behalf of Google, You will at all times meet or exceed all Applicable Data Protection Laws and Applicable Standards related to the collection, storage, accessing, and transmission of such data, including those established by PCI DSS. "**Cardholder Data**" means any primary account number, cardholder name, expiration date and/or service code, and security-related information (including but not limited to card validation codes/values, full track data, PINs, and PIN blocks) used to authenticate cardholders or authorize payment card transactions.

12. Suspension; Termination.

In addition to Google's suspension and termination rights in the Agreement, Google may: (a) immediately suspend Your access to Protected Information if (i) Google reasonably determines that You are not complying with this IPA; (ii) You are reasonably determined to be out of compliance with Applicable Data Protection Laws; or (iii) You have engaged in conduct that unreasonably prevents Google from timely curing an alleged violation of Applicable Data Protection Laws; or (b) terminate the Agreement if (i) Google reasonably determines that You have failed to cure material noncompliance with this IPA within a reasonable time; or (ii) Google reasonably believes it needs to do so to comply with Applicable Data Protection Laws or Applicable Standards.

13. Records; Destruction; Responding to Individual Requests; Sanitization.

13.1 Records and Appointment of a Qualified Data Protection Officer. You will maintain detailed, accurate, and up-to-date documentation and records relating to Your Processing of Personal Information sufficient to comply with this IPA and Applicable Data Protection Laws. Where required by Applicable Data Protection Laws, You will appoint and maintain a qualified data protection officer and make available the contact information of the data protection officer upon reasonable request.

13.2 Description of Processing. The Agreement, including relevant orders or statements of work associated with the Services, will specify the Processing activities,

subject matter, duration of Processing, categories of individuals, and the types and categories of Personal Information Processed, including any special categories of Personal Information or sensitive Personal Information.

13.3 Return or Deletion of Information. Upon the termination or expiration of the Agreement or the relevant order or statement of work for the Services, You will promptly: (a) return to Google all copies, whether in written, electronic or other form or media, of Personal Information in Your possession or the possession of Third Party Provider; and (b) where permitted, delete and render Protected Information unreadable in the course of disposal, securely dispose of all such hard copies, and where requested certify in writing Your compliance.

13.4 Subject Access Requests. Upon Google's reasonable request related to Google's obligations under Applicable Data Protection Laws, You will (i) promptly provide to Google a particular individual's Personal Information in an agreed upon format, and (ii) securely delete, modify, or correct a particular individual's Personal Information from Your records. If You are unable to delete the Personal Information for reasons permitted under the Applicable Data Protection Laws, You will (i) promptly inform Google of the reason(s) for Your refusal, including the legal basis of such refusal, (ii) ensure the ongoing privacy, confidentiality, and security of such Personal Information, and (iii) delete the Personal Information promptly after the expiry of the reason(s) for Your refusal. Unless You are acting as a Data Controller for the relevant request, You will notify Google of requests of individuals to exercise their legal rights with respect to the individual's Personal Information and not respond to such requests without Google's prior written authorization.

13.5 Sanitization. You will use a media sanitization process that deletes and destroys data in accordance with the U.S. Department of Commerce's National Institute of Standards and Technology's guidelines in NIST Special Publication 800-88 or alternative standard so long as Your data protection or other relevant officer certifies in writing that the standard provides an equivalent level of data sanitization.

14. Survival.

Your obligations under this IPA will survive expiration or termination of the Agreement and completion of the Services as long as You continue to have access to Protected Information.

15. Changes to the IPA.

15.1 Changes to URLs. Google may change any link or URL referenced in this IPA and the content at any such URL, except that Google may only:

(a) change the Applicable Standard Contractual Clauses in accordance with Section 15.2 (Changes to the IPA) or to incorporate any new version of the Applicable Standard Contractual Clauses that may be adopted under Applicable Data Protection Laws, in each case in a manner that does not affect the validity of the Applicable Standard Contractual Clauses; and

(b) make available a Data Transfer Solution in accordance with Section 15.2 (Changes to the IPA) or to incorporate any new versions of a Data Transfer Solutions that may be adopted under Applicable Data Protection Laws. For the purposes of this Section 15.1(b), Google may add a new URL and amend the content of such URL in order to make available such Data Transfer Solution.

(c) update and maintain relevant U.S. State Data Protection Laws in accordance with Section 15.2 (Changes to the IPA) or to incorporate any new U.S. State Data Protection Laws be adopted.

15.2 Changes to the IPA. Google may change this IPA if the change:

(a) is permitted by this IPA, including as described in Section 15.1 (Changes to URLs);

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

(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 IPA; and (iii) otherwise have a material adverse impact on the parties' rights under this IPA, as reasonably determined by Google.

16. Certification of Compliance.

You certify that You understand and will comply with all restrictions imposed upon Your Processing of Personal Information under the Agreement and applicable restrictions or limitations on Secondary Use of Personal Information as set forth in Applicable Data Protection Laws.

The following Parts B ("Process Outsourcing Requirements") and C ("HIPAA Business Associate Requirements") will apply to the extent applicable to the Services performed.

Part B: Process Outsourcing Requirements

1. Introduction.

You will comply with this Part B to the extent both of the following conditions apply: (i) Your personnel are provisioned with access to Protected Information on Google-owned or provisioned devices, systems, or endpoints and (ii) at least 15 of Your personnel will be providing services to Google from Your work location.

2. Additional Security Requirements.

2.1 Minimum Security Measures. You will implement the following minimum security requirements:

(a) an electronic, centrally-managed access control system with perimeter alarms on all doors giving access to the segregated area in which Services are performed;

(b) a badging process that identifies only Your personnel with a business need to access areas in which Services are performed;

(c) access control systems to record and store entry and exit details for all personnel and visitors to Your facilities for at least 30 days for common areas and 45 days for areas in which Services are performed;

(d) a CCTV system at facilities in which Services are performed with coverage sufficient to capture images of all Google assets and access/egress points, including emergency exits with lighting during hours of darkness;

(e) dedicated constant (24 hours per day, 365 days per year), on-site guarding at Your facilities in which Services are performed; and

(f) forced door alarms at facilities in which Services are performed, and door held alarms with default settings of 30 seconds or more.

2.2 Clean Room Security MeasuresClean Room Security Measures. You will perform Services in an enclosed area that is physically and logically separated from all other workflow processes that are not required for the provision of Services (including other Google workflows) and limited to Your authorized personnel ("**Clean Room**") and You will apply the following security requirements, in addition to those listed in Part B, Section 2.1, to any Clean Room:

(a) You will physically secure any Clean Room, including workspaces, from access by individuals not authorized by You to provide Services;

(b) You will logically separate networks, systems, and devices used for Services performed within a Clean Room from Your networks, systems, and devices used for other purposes;

(c) You will not remove any Google-managed hardware, software, or documentation from a Clean Room, except as required to perform Services and with Google's prior written approval;

(d) You will maintain reasonable logs of individuals with authorized access to any Clean Room;

(e) on request, You will give Google access to relevant access logs and CCTV images;

(f) You will not permit personal property in the Clean Room, including closed containers, bags, papers, purses, dongles, cameras, mobile phones, or other electronic devices;

(g) You may bring business equipment, including hardware or electronic devices into and out of the Clean Room only with prior written approval from the Google project manager identified in the statement of work for the Services, and only to the extent necessary to (i) secure and maintain any approved non-Google information technology; and (ii) reasonably comply with the Agreement; and

(h) You will otherwise comply with Google's written instructions in an applicable statement of work or other documentation (as may be updated from time-to-time).

3. Additional Internal Process Controls.

You will limit access to Protected Information to Your personnel and Third Party Providers who (i) have completed all Google-required training under the Agreement and as made available to You, including any legally-required training; and (ii) have agreed in writing at least once every calendar year to Your provider's confidentiality agreement.

4. Protected Information Incident Reimbursement.

4.1 Investigation and Remediation Costs. To the extent that You (including, for clarity, Your personnel, or Your Third Party Providers) are responsible for a Security Incident, or breach the Agreement or fail to notify Google in connection with a Security Incident, You will reimburse Google for any direct losses and expenses due to those acts or omissions, and pay Google its actual costs incurred to investigate and remediate the Security Incident.

4.2 Third Party Assessment. If more than one Security Incident occurs within any 90 day period, Google may require You to retain at Your cost a Google-approved, third-party security firm to assess Your Safeguards. You will, or will authorize the third party to, provide the resulting assessment report to Google. You will correct any vulnerabilities identified in any such assessment and where such assessment identifies critical or high findings, Google may in its discretion require You to conduct a reassessment (at Your cost) of Your Safeguards within 12 months following the third-party assessment to validate that any critical or high findings have been remediated.

4.3 Service Transition Costs. If Google determines that Your failure to comply with this IPA creates reasonable grounds to suspend Your access to Protected Information, information technology, or facilities, or to terminate the Agreement, You will reimburse Google for its reasonable costs in transitioning Services to another provider.

4.4 Incident Notices. If Google decides in its sole discretion to notify individuals affected by a Security Incident, You will reimburse Google for the reasonable costs of such notification, including (a) preparing and delivering notices; (b) establishing a call center hotline or other incident response communications procedures; (c) costs for one year of commercially reasonable credit-monitoring services that is acceptable to Google for affected individuals (or any alternative service required by Applicable Data Protection Laws, advisable under Applicable Standards, or requested by a Regulator); and (d) reasonable attorneys' and consultants' fees and expenses.

5. Process Outsourcing Assessment.

In addition to any other assessments permitted under the Agreement, Google may assess the adequacy of Your Safeguards under this Section 5.

5.1 Vulnerability Scans. If You are approved to Process Protected Information using non-Google network addresses, You must permit Google to perform regular vulnerability scans of all such addresses on a reasonable, recurring basis, provided that such scans may not be performed more frequently than once every 7 days. You will maintain an up-to-date list of non-Google network addresses and notify Google promptly of any changes to the list, including a written notice 15 days before releasing or transferring any such address to another tenant or owner.

5.2 Direct Tests. If Google decides, in its reasonable judgment, to directly test any non-Google information technology used to perform Services, Google and You will promptly develop a mutually-agreeable protocol that permits Google to adequately assess Your Safeguards.

6. Process Outsourcing Audits and Monitoring.

You expressly acknowledge and consent to auditing and monitoring by Google of all Your networks, applications, facilities, and workstreams used to perform Services, including all communication methods that You (including, for clarity, Your Third Party Providers) use to contact individual users in performing Services, including in-person, telephones, computers, electronic devices, and any other methods. Google's auditing and monitoring may include random on-site inspections of Your facilities, equipment, networks, or applications used to perform Services, and using quality control communications (including calls or messages) to confirm Your compliance with the Agreement.

7. Business Continuity.

7.1 Business Continuity Plan. You will develop and maintain a documented business continuity plan ("**BCP**") within 60 days of your initial provision of Services that: (i)

maintains Google's continued access to the Services; (ii) prevents the unintended loss or destruction of Protected Information; and (iii) ensures continued delivery of the Services to Google through any business disruption experienced by You. You will furnish the BCP to Google and update the BCP annually as needed.

7.2 Notification of BCP Invocation. If an event causes the BCP to be invoked, You will notify Google as soon as possible.

7.3 BCMS. You will implement or maintain a business continuity management system ("BCMS") that is in alignment with the ISO 22301 Standard. A compliant BCMS must demonstrate leadership, planning, support, operations, performance evaluation, and improvement.

7.4 Outage. If You encounter an interruption or outage of any aspect of the Service that impacts Google for any duration, You will furnish to Google a root cause analysis or post-mortem report that includes corrective actions and the timeframe for completion.

Part C: HIPAA Business Associate Requirements

1. Introduction.

You will comply with this Part C to the extent You Process health information protected under the Health Insurance Portability and Accountability Act ("**HIPAA**")in connection with the provision of Services.

2. Additional Definitions.

In this Part C, all capitalized terms not otherwise defined in the Agreement will have the definitions given to them by HIPAA, including the following:

(a) "**Breach**" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

(b) "**PHI**" has the same meaning as the term "protected health information" at 45 C.F.R. § 160.103.

(c) "**Security Incident**" has the same meaning as the term "security incident" at 45 C.F.R. §164.304.

3. HIPAA Business Associate Obligations.

Where required by HIPAA and, if not so required, where instructed by Google, You will in addition to the obligations in the IPA:

(a) not use or disclose PHI other than to perform Services in accordance with the Agreement or as required by law;

(b) use reasonable administrative, technical, and physical safeguards, and comply with the Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided by the Agreement;

(c) report to Google any use or disclosure of PHI not provided for by the Agreement or any Breach or Security Incident of which You become aware;

(d) ensure that any Third Party Providers that Process PHI on behalf of Google contractually agree to the same terms that apply to You with respect to such PHI;

(e) provide access to PHI maintained in a Designated Record Set in accordance with 45 C.F.R. § 164.524 and Google's specified timeframes;

(f) on Google's request, amend the PHI maintained in a Designated Record Set in accordance with 45 C.F.R. § 164.526;

(g) assist Google in responding to an Individual's request for an accounting of PHI disclosures in accordance with 45 C.F.R. § 164.528 and Google's specified timeframes;

(h) make Your internal practices and records available to the Secretary of the Department of Health and Human Services to determine HIPAA compliance; and

(i) return or destroy (and retain no copies of) all PHI received from Google once such PHI is not needed to perform Services.

Information Protection Addendum Version 11

Last Updated June 5, 2024

Previous Versions

- Version 10 - September 23, 2023
- Version 9 - October 5, 2022
- Version 8 - October 27, 2021