Information Protection Addendum

Version 13

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 (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"**).

(b) Part C (Google Cloud Requirements) of this IPA will apply to the extent that You provide Services in connection with a "Service" as defined in the then-current "Cloud Data Processing Addendum" at https://cloud.google.com/terms/data-processing-addendum (**"Google Cloud Products"**) or if indicated in a SOW.

(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.

(d) Physical Access & Facility Standards will apply to the extent You Process Protected Information from a location not controlled by

Google and Your personnel are provisioned with access to Protected Information on Google-owned or provisioned devices, systems, or endpoints.

2. Definitions; Interpretation.

2.1 Definitions. In this IPA:

(a) "**Adequate Country**" means: (a) for data processed subject to the EU GDPR: the EEA, or a country or territory recognized as ensuring adequate data protection under the EU GDPR, other than on the basis of an optional data protection framework; (b) for data processed subject to the UK GDPR: the UK or a country or territory recognized as ensuring adequate data protection under the UK GDPR and the Data Protection Act 2018, other than on the basis of an optional data protection framework; (c) for data processed subject to the Swiss FDPA: 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, or (ii) recognized as ensuring adequate data protection by the Swiss Federal Council under the Swiss FDPA, in each case, other than on the basis of an optional data protection framework; and/or (d) for data processed subject to any other Applicable Data Protection Laws, the jurisdiction in which such Applicable Data Protection Laws apply or a country or territory recognized as ensuring adequate or appropriate data protection under such Applicable Data Protection Laws, other than on the basis of an optional data protection framework.

(b) "**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).

(c) "**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, LGPD, HIPAA, GLBA, European Data Protection Law, U.S. State Data Protection Laws, and rules that govern the processing of Bulk Sensitive Data.

(d) "**Applicable Standard Contractual Clauses**" means the standard data protection clauses, including the Controller - Controller Standard Contractual Clauses (SCCs), Controller - Processor SCCs and Processor - Processor SCCs, at

https://business.safety.google/applicablesccs (as may be updated in accordance with Section 16 (Changes to the IPA) of this IPA).

(e) "**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**").

(f) "**Bulk Sensitive Data**" means bulk U.S. sensitive personal data or government-related data, each as defined in 28 C.F.R. Part 202 on Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons.

(g) "**Confidential Information**" either:

(i) has the meaning given in the Agreement; or

(ii) if no such meaning is given, means information that one party (or its Affiliate) discloses to the other party under the Agreement and that is marked as confidential or would normally be considered confidential information under the circumstances. Confidential Information 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.

(h) "**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" or "business" as defined by Applicable Data Protection Laws.

(i) "**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.

(j) "**Data Transfer Solution**" means a solution, other than the Applicable Standard Contractual Clauses, 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.

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

(l) "**European Data Protection Law**" means, as applicable: (i) the GDPR; and/or (ii) the Swiss FDPA.

(m) "**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 amended and incorporated into United Kingdom law by the European Union (Withdrawal) Act 2018 and applicable secondary legislation made under that Act ("**UK GDPR**"), (each as amended, superseded, or replaced).

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

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

(p) "**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.

(q) "**Google Customer**" means a direct or indirect customer or partner of a Google Entity who is a Data Controller or Data Processor of Personal Information Processed by You. "Google Customer" does not include individuals.

(r) "**Google Customer Data**" means data provided to You by or on behalf of a Google Entity or Google Customer (and data derived from such data) that You Process on behalf of a Google Customer.

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

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

(u) "**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.

(v) “**LGPD**” means Brazilian Law 13,709 for the protection of personal data.

(w) “**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).

(x) “**Personal Information**” means (a) any information that is Processed in connection with the Services and (i) that is about an individual or (ii) that is not specifically about an individual but, when combined with other information, may identify an individual, and (b) any other information that constitutes “personal data” or “personal information” within the meaning of Applicable Data Protection Laws. “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.

(y) “**Physical Access & Facility Standards**” means the standards for vendors and suppliers providing services from physical worksite locations as set forth in the most recent version of the Physical Access & Facility Standards available at (https://support.google.com/guideforextendedworkforce/answer/14554952?hl=en&ref_topic=13315988&sjid=11652430901285768499-NC).

(z) “**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 GDPR.

(aa) “**Protected Information**” means Personal Information, De-identified Data, Google Customer Data or any confidential information (as marked by the parties or defined in the Agreement as Confidential Information) that You 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.

(bb) "**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.

(cc) "**Required Subprocessor Information**" means the name and address of the Subprocessor, the Processing activity that the Subprocessors will perform, the location (country and region) where the Subprocessor will Process Protected Information and a point of contact and contact details (e.g. email address) for the Subprocessor to receive queries about Processing Protected Information from Google or the Data Controller.

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

(ee) "**Safeguards**" means the technical, organizational, administrative, and physical controls described in Section 6 (Safeguards), Section 7 (Encryption Requirements), Section 8 (Use of Google Networks, Systems, or Devices), Section 9.3 (Your Continuous Self-Assessment), Section 10.1 (Security Incident Response Program), and Section 12 (PCI Compliance).

(ff) "**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.

(gg) "**Security Incident**" means: (i) 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, or (ii) a breach of the security of Your systems, devices, networks or facilities that has or would be reasonably

likely to have a material adverse impact on the authenticity, integrity, availability or confidentiality of the Services. Security Incidents do not include unsuccessful access attempts or attacks that do not compromise the confidentiality, integrity, or availability of Protected Information or the Services, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(hh) "**Services**" means any goods or services that You provide to or for Google under the Agreement.

(ii) "**SOW**" will have the meaning given to it in the Agreement or, where such definition is not specified, will mean a statement of work (if any) entered under the Agreement.

(jj) "**Subprocessor**" means any third party (including Your Affiliates) authorized to Process Protected Information on Your behalf in connection with the Services regardless of whether You engage them directly or You authorize Your Subprocessors to engage them. "Subprocessor" includes "subprocessor" within the meaning of the Applicable Standard Contractual Clauses.

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

(ll) "**Swiss FDPA**" means, as applicable, the Federal Data Protection Act of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Data Protection Act of 14 June 1993), or the revised Federal Data Protection Act of 25 September 2020 (with the Ordinance to the Federal Data Protection Act of 31 August 2022).

(mm) "**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.

(nn) "**You**" or "**Your**" means the party (including any personnel, contractor, or agent acting on behalf of such party) that performs Services for a Google Entity under the Agreement. References to "You" and "Your" include any Subprocessors and (if applicable) Material Subcontractors (as defined in Part C).

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 Processing Roles. Google, a Google Entity or a Google Customer is the Data Controller of Personal Information. 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.

3.2 General Obligations. When You Process Protected Information, You will at all times:

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

(b) except where Section 3.3 (Obligations Where You Process Personal Information as a Data Controller) applies, Process Protected Information only on behalf of the Data Controller and in accordance, and only as strictly necessary to comply, with the limited and specified purposes of Processing, business purpose, and instructions stated in the Agreement or other written instructions given by Google Entities, 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;

(d) to the extent permitted by applicable law, promptly notify Google if You receive a communication from a Regulator regarding Protected Information or Your provision of Services to Google, provide Google a reasonable summary of the communication and assist Google in responding to the communication in respect of Your Processing of Protected Information;

(e) promptly notify Google if You believe (i) compliance with this IPA (including any instructions given by Google Entities) will interfere with your obligations under Applicable Data Protection Laws; or (ii) You can no longer meet Your obligations under this IPA.

3.3 Obligations Where You Process Personal Information as a Data Controller. If permitted by Section 3.1 (Processing Roles) 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 6.5), 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. Data Location and Transfers

4.1 Data Location. You will only Process Protected Information in locations (country and region) authorized by Google either: (a) in the SOW; or (b) in writing in response to a request sent by You to subprocessor-compliance@google.com. You will provide Google with the address of these locations on request. You will maintain accurate information about the location (country and region) where You and Your Subprocessors Process Protected Information and make this information available to Google upon request.

4.2 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.

(b) To the extent either party transfers Personal Information subject to the GDPR or other Applicable Data Protection Laws, and the party receiving the Personal Information is not (i) located in an Adequate Country, or (ii) already subject to binding obligations under a valid Data Transfer Solution with respect to the relevant transfers, the parties expressly agree to comply with a Data Transfer Solution, where applicable, with respect to the transfers or, where a Data Transfer Solution is not applicable, to enter into the Applicable Standard Contractual Clauses with respect to the transfers as further detailed in Sections 4.2(c) and (d) below.

(c) To the extent Personal Information is transferred pursuant to the Applicable Standard Contractual Clauses and You Process that 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, Processor - Processor SCCs, or other SCCs (as applicable) with respect to the relevant transfers.

(d) To the extent Personal Information is transferred 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 with respect to the relevant transfers.

(e) To the extent either party Processes Personal Information transferred in accordance with a Data Transfer Solution, the party receiving that 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 the 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 the 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.

4.3 Google Controller. 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.

5. Subprocessors.

5.1 Authorization for Subprocessor Engagement. You may not engage a Subprocessor (or authorize Your Subprocessor to engage any further Subprocessor) without Google's prior written authorization. You will send any requests for Google's authorization to subprocessor-compliance@google.com or the webform available at https://sites.google.com/corp/view/subprocessor-notifications/home at least 6 months before the Subprocessor starts Processing Protected Information. Your request must include the Required Subprocessor Information.

5.2 Your Subprocessor Obligations. If You engage or authorize a Subprocessor, You will:

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

(b) engage Your Subprocessor pursuant to a written contract that imposes the same restrictions and obligations (including regarding further subprocessors) with respect to the processing of Protected Information that are required of You under this IPA;

(c) monitor Your Subprocessors and be responsible for Your Subprocessors' acts and omissions in connection with the Services;

(d) on Google's request, promptly provide Google with information about any Subprocessor, including a description of contractual terms with the Subprocessor and information about the due diligence and periodic reviews of the Subprocessor;

(e) publish and maintain a list of Your Subprocessors, including the Required Subprocessor Information, on Your website and ensure that Your Subprocessors do the same on their website for any further Subprocessors that they engage or authorize);

(f) notify Google by email to subprocessor-compliance@google.com if a Subprocessor engagement ends or the Required Subprocessor Information changes. You will provide at least 6 months' prior notice of changes to a

Subprocessor's Processing activity or location (country or region) ("Significant Subprocessor Change") and prompt notice in all other cases. If Google objects to a Significant Subprocessor Change, then on Google's written request, You will discuss any concerns with Google and give good faith consideration to those concerns and appropriate ways to address them. If You are unable to address Google's concerns, then either: (i) You will not make the change, or (ii) Google may terminate the Agreement or the relevant SOW without liability.

5.3 Subprocessor Transparency. If required to address Applicable Data Protection Laws, Google Entities may disclose the information You provide under this Section 5 to Google Customers, Data Controllers and Regulators.

6. 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:

6.1 Physical Controls. To the extent You Process Protected Information in facilities not managed by a Google Entity or Google Customer, 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.

6.2 Technical Controls. To the extent You Process Protected Information on systems not owned and controlled by a Google Entity or Google Customer, 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.

6.3 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.

6.4 Supplemental Supplier and Partner Security Standards for Software Development. 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.

6.5 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 6.5, until You remedy such failure.

6.6 Additional Safeguards for Process Outsourcing. To the extent You Process Protected Information from a location not controlled by Google and Your personnel are provisioned with access to Protected Information on Google-owned or provisioned devices, systems, or endpoints, You will:

(a) Physical Access & Facility Standards. You will implement and maintain the requirements described in the Physical Access & Facility Standards, including that You will perform Services in an

enclosed area that is (i) physically and logically separated from all other workflow processes that are not required for the provision of Services (including other Google workflows) and (ii) limited to Your authorized personnel; and

(b) Business Continuity and Disaster Recovery.

(i) BCMS. You will implement and maintain an appropriate business continuity management system ("**BCMS**") that is aligned with ISO 22301 or another internationally recognised standard. Your BCMS will demonstrate leadership, planning, support, operations, performance evaluation, and improvement.

(ii) BCDR Plan. You will develop, maintain, and regularly review a business continuity and disaster recovery plan ("**BCDR Plan**"). The BCDR Plan will (a) address how You will anticipate, withstand, respond to, and recover from events that disrupt the operations and resources required to provide the Services, and (b) contain appropriate service levels and recovery time objectives. Upon request you will provide Google Your then-current BCDR Plan.

(iii) Training and Personnel. You will ensure relevant personnel: (a) are appropriately and regularly trained in Your BCDR Plan, and (b) if needed participate in security awareness, operational resilience, business continuity and disaster recovery training organized by Google. You will maintain, and provide to Google upon request, an up-to-date list, including names and emergency phone numbers, of personnel who will be primary and secondary contacts for Google to communicate with directly if there is an incident identified by You or Google requiring or resulting in implementation of any portion of Your BCDR Plan.

(iv) Communication. You will notify Google without undue delay if: (a) You make a material change to Your BCDR Plan, or (b) You activate Your BCDR Plan.

(v) Outage. If there is a disruption or outage of any aspect of the Service that impacts Google, You will: (a) promptly notify Google; and (b) without undue delay provide Google a root cause analysis that includes corrective actions and the timeframe for completion.

7. Encryption Requirements.

You will use a modern, maintained, and industry-standard means of encryption to protect Protected Information in transit between systems and at rest on Your systems including online data storages and backups.

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

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

9. Assessments; Audits; Correcting Vulnerabilities.

9.1 Data Protection Assessments. Upon Google's written request, You will promptly and accurately complete any assessment of Your compliance with this IPA, Applicable Data Protection Laws, the MVSP, or Applicable Standards provided by Google. 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.

9.2 Penetration Testing. If You Process Protected Information on Your systems, or Your systems connect to Google's or a Google Customer's internal systems, then:

(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 9.2(a), 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 if the testing is criteria is 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 9 as Your Confidential Information.

For the purpose of this Section 9.2, Google will agree to test Your systems in a non-production environment, so long as You provide reasonable evidence that the testing environment is similar to the production environment in functionality.

9.3 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.

9.4 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 9.4 will not reduce or suspend Your obligations under Sections 10 (Security Incident Response) and 14

(Records; Destruction; Responding to Individual Requests; Sanitization) or Google's rights under Section 13 (Suspension; Termination).

9.5 Data Protection Audits.

(a) Audits and Certifications. Upon written request by Google, not more than once per year, Google (or Google's independent third party assessor that is not Your competitor) 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 9.4(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.

(c) Findings. If an audit results in any findings, You will, within the time frame Google reasonably requires based on the criticality of the finding: (a) submit a remediation response plan to address the finding to Google for review; (b) implement the response plan with any changes Google reasonably requires to close the finding; and (c) provide Google with periodic updates on the status of the remediation activity until the response plan is fully executed and the finding is closed.

9.6 Other Confidential Information. Google will take reasonable efforts to protect confidential information that You make available to Google under this Section 9 in accordance with the applicable confidentiality terms entered into between the parties.

10. Security Incident Response.

10.1 Security Incident Response Program.

(a) Program. You will maintain a reasonable Security Incident response program that includes plans and procedures that You will follow to respond to or recover from Security Incidents and facilitate effective communication with impacted parties ("Incident Response Program").

(b) Testing. You will: (i) test Your Incident Response Program at least annually; (ii) promptly remediate all issues identified during testing; and (iii) if needed update Your Incident Response Program. Upon request, You will: (x) provide Google the results of Your Incident Response Program testing and any remediation plans; and (y) participate in Security Incident response exercises organized by Google and remediate all issues identified during such exercises.

(c) Training. You will ensure relevant personnel: (ii) are appropriately and regularly trained in Your Incident Response Program, and (ii) if needed participate in Security Incident response training organized by Google.

10.2 Security Incident Notification.

(a) If You become aware of a Security Incident, You will promptly: (i) stop the unauthorized access; (ii) secure Protected Information and Your systems, devices, networks and facilities (as applicable); (iii) notify Google without undue delay (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 10.2(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. You will promptly notify Google if there is a material change to any information that You have previously communicated to Google about the Security Incident.

10.3 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 impacted parties or Regulators 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.

10.4 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 or Google Customer, unless Google provides its explicit written authorization.

11. 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.

12. PCI Compliance.

To the extent You receive, process, transmit, or store any Cardholder Data for or on behalf of a Google Entity or Google Customer, 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.

13. 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 or the relevant SOW if (i) Google reasonably determines that You have failed to cure material noncompliance with this IPA within a reasonable time; (ii) Google objects to a Subprocessor or (if applicable) Material Subcontractor (as the term is defined in Part C); or (iii) Google reasonably believes it needs to do so to comply with Applicable Data Protection Laws or Applicable Standards.

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

14.1 Records; Appointment of a Qualified Data Protection Officer; Point of Contact; Evidence of Processing Terms.

(a) Records. 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 and make those records available to Google upon request.

(b) Appointment of a Qualified Data Protection Officer. 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 to Google upon request.

(c) Point of Contact. You will maintain a point of contact to receive queries about Processing Protected Information from Google or the Data Controller and make available the contact information for that point of contact available to Google upon request. You will promptly notify Google by email to subprocessor-compliance@google.com if You change Your point of contact. Google may publish information about Your point of contact on Google's website.

(d) Evidence of Processing Terms. Google Entities may disclose the Agreement to Google Customers, Data Controllers or Regulators to establish that appropriate contractual provisions are in place for Your Processing of Protected Information.

14.2 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.

14.3 Return or Deletion of Information. Upon Google's request, or the termination or expiration of the Agreement or the relevant order or statement of work for the Services, You will: (a) return to Google all or any copies, whether in written, electronic or other form or media, of Protected Information in Your possession 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, in each case as soon as reasonably practicable and within a maximum period of 90 days.

14.4 Subject Access Requests. Upon Google's reasonable request, You will promptly take all reasonable steps to effectuate an individual data subject access request related to Google's obligations under Applicable Data Protection Laws as directed by Google. If You are unable to take directed actions, 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 (i) notify Google of requests of individuals to exercise their legal rights with respect to the individual's Personal Information (ii) notify Google of any complaints You receive regarding an individual's Personal Information and (iii) not respond to such requests without Google's prior written authorization.

14.5 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.

15. 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 Process Protected Information.

16. Changes to the IPA.

16.1 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 16.2 (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 16.2 (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 16.1(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 16.1 (Changes to the IPA) or to incorporate any new U.S. State Data Protection Laws adopted.

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

(a) is permitted by this IPA, including as described in Section 16.1 (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.

16.3 Applicable IPA Version. If changes are made to the IPA, the new version of the IPA will be posted at https://business.safety.google/ipa, and the replaced version will be added to a dated archive available on that

webpage. Except for those updates authorized under Section 16 (Changes to the IPA), the version of the IPA current as of the date You (i) executed a contract with Google incorporating the IPA or (ii) clicked to accept the terms of this IPA, is the version of the IPA that applies to Your Agreement.

17. Certification of Compliance with Applicable Data Protection Laws.

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, including prohibitions on transactions involving Bulk Sensitive Data.

Part B: HIPAA Business Associate Requirements

1. Introduction.

You will comply with this Part B 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 B, 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.

Part C: Google Cloud Requirements

1. Introduction.

You will comply with this Part C to the extent that You provide Services in connection with a "Service" as defined in the then-current "Cloud Data Processing Addendum" at https://cloud.google.com/terms/data-processing-addendum ("**Google Cloud Product**") or if indicated in a SOW.

2. Additional Definitions.

2.1 Definitions. In this Part C of the IPA:

(a) "**ICT**" means information and communication technology.

(b) "**ICT Service**" means a service listed in Annex 1 of Part C of this IPA.

(c) "**Legal Entity Identifier**" means a valid and active legal entity identifier as described in the implementing technical standards on the register of information developed pursuant to Article 28(9) of Regulation (EU) 2022/2554 (known as the EU Digital Operational Resilience Act or DORA).

(d) "**Material Subcontractor**" means any third party (including Your Affiliates) that: (a) provides supports the Services that You provide to Google, or (b) is otherwise essential to Your delivery of the Services to Google, regardless of whether You engage them directly or You authorize Your Material Subcontractors to engage them. "Material Subcontractors" include, but are not limited to, Subprocessors.

(e) "**Regulated Google Cloud Customer**" means a direct or indirect customer or partner of a Google Entity that operates in a regulated sector and benefits from the Services in connection with a Google Cloud Product (including any appointee acting on their behalf).

(f) "**Regulator**" means an entity with supervisory or regulatory authority over a Google Entity or Regulated Google Cloud Customer under applicable law (including any appointee acting on their behalf).

(g) "**Required Subcontractor Information**" means the name, address, country of registration and Legal Entity Identifier of the Material Subcontractor and its ultimate parent company, the activity (and where applicable the ICT Service(s)) that the Material Subcontractor will perform and the location (country and region) where the Material Subcontractor will perform the activity.

3. Corporate Information.

You will promptly provide the following information to Google upon request: Your full legal name, Your registered office, Your country of registration, Your company number, Your Legal Entity Identifier, Your parent company (if applicable), and, if You are authorized by, registered with, or subject to supervision or oversight by a financial sector supervisory authority, details of Your supervisory authority. Google Entities may disclose this information and a general description of the

Services to third parties. You will notify Google by email to subcontractor-changes@google.com if any such information changes no later than 30 days after the change takes effect.

4. Monitoring.

You will cooperate with Google's diligence and monitoring of Your performance of the Services (including any service levels) and provide Google the information it reasonably requests to effectively perform such activities. If Google identifies any risk or performance issues, You will, within the time frame Google reasonably requires based on the criticality of the issue: (a) submit a remediation response plan to address the issue to Google for review; (b) implement the response plan with any changes Google reasonably requires to address the issue; and (c) provide Google with periodic updates on the status of the remediation activity with associated evidence until the response plan is fully executed and the issue is addressed. Google Entities may disclose the results of Google's diligence and monitoring activities to Regulated Google Cloud Customers and Regulators.

5. Secrecy Notice.

Protected Information may include information that is subject to secrecy and confidentiality laws and regulations in certain countries. Under those laws and regulations, unauthorized disclosure or exploitation of such information is a criminal offense and may be punishable by imprisonment. There are increased penalties if an offense is committed with the intention of financial gain (including in favor of third parties) or causing damage. You will ensure that all personnel who Process Protected Information on Your behalf are provided equivalent notice as is provided to You in this Section.

6. Authorized Locations.

You will only perform the Services in locations (country and region) authorized by Google either: (a) in the SOW; or (b) in writing in response to a request sent by You to subcontractor-changes@google.com. You will provide Google with the address of these locations on request. Google Entities may disclose this information to Regulated Google Cloud Customers and Regulators.

7. Material Subcontractors

7.1 Authorization for Material Subcontractor Engagement. You may not engage a Material Subcontractor (or authorize your Material

Subcontractor to engage any further Material Subcontractor) without Google's prior written authorization. You will send any requests for Google's authorization to subcontractor-changes@google.com at least 6 months before the Material Subcontractor starts performing the Services. Your request must include the Required Subcontractor Information.

7.2 Your Material Subcontractor Obligations: If You engage or authorize a Material Subcontractor, You will:

(a) carry out adequate due diligence of Your Material Subcontractor to ensure its capability of providing the subcontracted obligations in accordance with the Agreement, including this IPA, and annually review such Material Subcontractor to ensure it maintains such capability;

(b) engage Your Material Subcontractor pursuant to a written contract that imposes the same obligations (including regarding audit and subcontracting) with respect to the subcontracted obligations that are required of You under this IPA;

(c) monitor Your Material Subcontractors and be responsible for Your Material Subcontractors' acts and omissions in connection with the Services;

(d) on Google's request, promptly provide Google with information about any Material Subcontractor, including a description of contractual terms with the Material Subcontractor and information about the due diligence and periodic reviews of the Material Subcontractor;

(e) on Google's request, promptly provide Google a list of Your Material Subcontractors, including the Required Subcontractor Information, and ensure that Your Material Subcontractors do the same for any further Material Subcontractors that they engage or authorize); and

(f) notify Google by email to subcontractor-changes@google.com if a Material Subcontractor engagement ends or the Required Subcontractor Information changes. You will provide at least 6 months' prior notice of changes to a Material Subcontractor's activity, ICT Service(s) (where applicable) or location (country or region) ("Material Subcontractor Change") and prompt notice in all other cases. If Google objects to a Material Subcontractor Change, then on Google's written request You will discuss any concerns with Google and give good faith consideration to those concerns and appropriate ways to address them. If You are unable to address Google's concerns, then either: (i) You will

not make the change, or (ii) Google may terminate the Agreement or the relevant SOW without liability.

7.3 Material Subcontractor Transparency. Google Entities may disclose the information You provide under this Section 7 to Regulated Google Cloud Customers and Regulators.

8. Penetration Testing

8.1 If You Process Protected Information on Your systems, or Your systems connect to Google's or a Google Customer's internal systems, then in addition to the requirements under "Penetration Testing" Section of Part A of this IPA and only where required to address applicable law:

(a) Google Entities may disclose the results of such penetration tests to Regulated Google Cloud Customers and Regulators;

(b) Google may permit Regulated Google Cloud Customers and Regulators to participate in penetration tests conducted by or on behalf of Google or if required by applicable law perform their own penetration tests; and

(c) If applicable law requires testing in production environments, Google will use reasonable efforts to satisfy Regulated Google Cloud Customers and Regulators using tests in a non-production environment. If this is not sufficient, You will permit testing in production environments provided that testers comply with Your reasonable safeguards.

9. Certifications and Audit Reports

9.1 You will maintain at least the following for the Services during the Term: (a) an ISO 27001 certificate; (b) a SOC 2 report; and (c) any other third party certification or report that You agree to obtain in the relevant SOW or that is required under applicable law (together the "Compliance Certifications"). Your Compliance Certifications will cover all the locations from which You provide the Services, be produced by a qualified and independent third party auditor following an audit, and be updated annually.

9.2 You will make Your Compliance Certifications and all corresponding reports (including, in the case of Your SOC 2 report, Your type II report) available for review by Google, Regulated Google Cloud Customers and Regulators upon request.

9.3 If a key system or control applicable to the Services is not covered in Your Compliance Certifications, You will on Google's request expand the scope of Your next Compliance Certification to cover such key system or control

10. Audits

10.1 Mandatory Audits. Applicable law, frameworks or mandatory contract terms may require a Regulated Google Cloud Customer or a Regulator to have the right to oversee, audit or inspect the Services or Your compliance with the Agreement. If a Regulated Google Cloud Customer or Regulator exercises such a right, Google will use reasonable efforts to satisfy the request itself, including by using the results of audits conducted by or on behalf of Google. If this is insufficient, You will reasonably cooperate and assist Google with such oversight, audits or inspections in accordance with applicable law, including by permitting Google, the Regulated Google Cloud Customer or the Regulator to: (a) review information that is necessary to demonstrate Your operations and controls for the Services and Your compliance with the Agreement and discuss such information with Your personnel, and (b) access Your premises used to provide the Services.

10.2 Protections. Activities under this Section will be conducted during business hours. When conducting activities under this Section, Google will:

(a) use reasonable efforts to minimize the disruption to You;

(b) where it is within Google's control, provide You two weeks' advance notice. Where Google is unable to provide two weeks' advance notice, Google will provide as much advance notice as reasonably possible; and

(c) be responsible for the acts or omissions of Regulated Google Cloud Customers. Nothing in this Section will require You to disclose or provide access to any of Your other customers' information or any premises not used to provide the Services to Google.

10.3 Findings. If an activity under this Section results in any findings (including binding Regulator recommendations), You will, within the time frame Google reasonably requires based on the criticality of the finding: (a) submit a remediation response plan to address the finding to Google for review; (b) implement the response plan with any changes Google reasonably requires to close the finding; and (c) provide Google with periodic updates on the status of the remediation activity with

associated evidence until the response plan is fully executed and the finding is closed.

11. Additional Background Checks

The Attachment B “Background Checks” of the Agreement is supplemented as follows:

11.1 Ineligibility. To the extent permitted under applicable law, personnel may not perform any Services if a background check reveals the personnel has in the previous 7 years: (a) been convicted of any criminal offense involving dishonesty or breach of trust or money laundering; or (b) agreed to enter into a pretrial diversion or similar program in connection with a prosecution for an offense in (a)

11.2 Maintenance. To the extent permitted under applicable law, You will re-perform the criminal court checks required under the Agreement for each personnel every 2 years and take such steps as required by the Agreement based on the results. If personnel have not had such checks re-performed within 2 years of their previous check, then You will restrict them from performing the Services until the background checks have been completed and confirm they remain eligible to perform the Services.

11.3 Evidence. Google Entities may disclose information that You provide to verify that You have conducted background checks to Regulated Google Cloud Customers and Regulators.

12. Business Continuity and Disaster Recovery

12.1 BCMS. You will implement and maintain an appropriate business continuity management system (“**BCMS**”) that is aligned with ISO 22301 or another internationally recognised standard. Your BCMS will include appropriate documented and up-to-date policies, procedures, business impact assessments and risk assessments and demonstrate leadership, planning, support, operations, performance evaluation, and improvement.

12.2 BCDR Plan. You will develop, maintain, and regularly review a business continuity and disaster recovery plan (“**BCDR Plan**”). The BCDR Plan will (a) address how You will anticipate, withstand, respond to, and recover from events that disrupt the operations and resources required to provide the Services, and (b) contain appropriate service levels and recovery time objectives. Upon request you will provide Google Your then-current BCDR Plan.

12.3 Testing. You will: (a) test Your BCDR Plan at least annually; (b) promptly remediate all issues identified during testing; and (c) if needed update Your BCDR Plan. Upon request, You will: (i) provide Google the results of Your BCDR Plan testing and any remediation plans; and (ii) permit Google to participate in Your BCDR Plan testing that is relevant to Google, and (iii) participate in business continuity and disaster recovery exercises organized by Google and remediate all issues identified during testing.

12.4 Training and Personnel. You will ensure relevant personnel: (a) are appropriately and regularly trained in Your BCDR Plan, and (b) if needed participate in security awareness, operational resilience, business continuity and disaster recovery training organized by Google. You will maintain, and provide to Google upon request, an up-to-date list, including names and emergency phone numbers, of personnel who will be primary and secondary contacts for Google to communicate with directly if there is an incident identified by You or Google requiring or resulting in implementation of any portion of Your BCDR Plan.

12.5 Communication. You will notify Google without undue delay if: (a) You make a material change to Your BCDR Plan, or (b) You activate Your BCDR Plan. Google Entities may disclose Your BCDR Plan, test results and remediation plans to Regulated Google Cloud Customers and Regulators.

12.6 Outage. If there is a disruption or outage of any aspect of the Service that impacts Google, You will: (a) promptly notify Google; and (b) without undue delay provide Google a root cause analysis that includes corrective actions and the timeframe for completion. Google Entities may disclose this analysis to Regulated Google Cloud Customers and Regulators.

12.7 Dependency Mapping. You will identify and document the resources (including people, assets, services and technology) that are essential to deliver, support and maintain the Services ("**Dependency Mapping**"). Your Dependency Mapping will identify (a) interconnections between resources, and (b) concentrations or single-points-of-failure. You will mitigate interconnection risks and concentration risks identified via Your Dependency Mapping. You will update Your Dependency Mapping at least annually and promptly following a significant change to essential resources. Upon request You will provide Google Your then-current Dependency Mapping and any mitigation plans. Google Entities may disclose Your Dependency Mapping or mitigation plans to Regulated Google Cloud Customers and Regulators.

13. Transition.

You will continue to provide the Services in accordance with the terms of the Agreement (including any applicable fees) [Fallback: for up to 12/24 months] after termination or expiration of the Agreement or SOW if required to enable Google or a Regulated Google Cloud Customer to transition away from the Services in compliance with applicable law ("**Transition Term**"). You will reasonably cooperate with Google during the Transition Term to transition Regulated Google Cloud Customers away from the Services. [**Fallback**: This "Transition" section can be deleted if Google has vendor redundancy (ex, the service provider is one of several providing the same service such that if one service provider terminates there is no knock-on impact to Google's ability to provide the services to our customers). It cannot be deleted if the service provider is the only one that provides the specific services, i.e., there is no vendor redundancy.]

14. Financial Sector Requirements

14.1 Authorized Recipient for BaFin (Germany). Under the German Financial Market Integrity Strengthening Act (Finanzmarktintegritätsstärkungsgesetz) ("FISG") Regulated Google Cloud Customers supervised by the German Bundesanstalt für Finanzdienstleistungsaufsicht ("BaFin") must identify an authorized recipient for notices from BaFin for their service providers if the provider's registered address is outside the European Economic Area. This requirement applies to the Regulated Google Cloud Customer's direct service providers and any relevant subcontractors, including You. If Your registered address is not in the European Economic Area, then You authorize Google Germany GmbH to receive notifications on Your behalf from BaFin in respect of Services that are used by or benefit Regulated Google Cloud Customers supervised by BaFin. [Fallback: Delete this "Authorized Recipient for BaFin (Germany)" section if provider's registered address is in the EEA]

14.2 Critical Third Parties (UK). Under the Financial Services and Markets Act 2000 (as amended) ("FSMA ") entities designated as critical third parties ("CTP") must inform relevant providers in their supply chain of the duties that apply to CTPs ("CTP Duties") under FSMA and the rules issued by the Bank of England, the Financial Conduct Authority and the Prudential Regulation Authority (together, the "UK Financial Regulators"). The UK Financial Regulators have explained the CTP Duties in Supervisory Statement (SS) 6/24. You acknowledge the CTP Duties and will inform Your Material Subcontractors of the CTP Duties. If a Google Entity is designated a CTP, You will reasonably cooperate and ensure Your Material Subcontractors reasonably cooperate with Google Entities and the UK Financial Regulators where necessary to meet those duties and solely in respect of the Services. For the avoidance of doubt, the CTP

Duties do not apply to You directly unless You are separately designated a CTP.

15. Public Sector Requirements.

This section addresses requirements that apply to Regulated Google Cloud Customers in the public sector ("Public Sector Customers ").

15.1 Freedom of Information Requests. Public Sector Customers are subject to government transparency and public disclosure laws and regulations, including the US Freedom of Information Act 1966 and the UK Freedom of Information Act 2000, and are required to include equivalent requirements in their contracts with their service providers ("**Transparency Obligations**"). You will reasonably cooperate with Google and Public Sector Customers in respect of the Transparency Obligations. Google Entities may disclose Your confidential information to Public Sector Customers if and only to the extent necessary to comply with Transparency Obligations.

15.2 Record Keeping. Public Sector Customers are subject to enhanced record-keeping rules. To enable Public Sector Customers to comply with these rules and subject to applicable laws, You will maintain and make available upon request to Google, Public Sector Customers or the Regulator, the records required under the Agreement for at least 5 years after termination or expiry of the Agreement or the relevant SOW.

15.3 Modern Slavery and Anti-bribery. Public Sector Customers are subject to enhanced modern slavery and anti-bribery rules. To enable Public Sector Customers to comply with these rules, You will promptly notify Google in writing if You suspect that You have breached, are breaching or are likely to breach applicable (a) anti-slavery and human trafficking laws and regulations, including the UK Modern Slavery Act 2015, or (b) commercial and public anti-bribery laws, including the U.S. Foreign Corrupt Practices Act of 1977 and the UK Bribery Act of 2010, which prohibits 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.

15.4 US Public Sector Requirements. Google provides products and services to United States federal government customers, and accordingly must flow down applicable Federal Acquisition Regulation ("**FAR**") and Defense Federal Acquisition Regulation Supplement ("**DFARS**") clauses. Where the Services are used for performance of a United States federal government contract, then the following FAR and DFARS, and their successor clauses, are incorporated by reference into Part C of this IPA: https://cloud.google.com/terms/cloud-us-reg-flowdowns?hl=en.

16. Confidential Disclosures.

Google Entities may disclose the Agreement to Regulated Google Cloud Customers or Regulators if required to address applicable law. If a Google Entity discloses the Agreement or Your Confidential Information (or authorizes Your Confidential Information to be disclosed) to Regulated Google Cloud Customers or Regulators under Part C of this IPA, Google will ensure that:

16.1 the Regulated Google Cloud Customer is subject to appropriate confidentiality obligations in respect of such information; and

16.2 the Regulator is notified of the confidential nature of such information and requested to keep it confidential under applicable law.

17. Changes in Law.

The laws, regulations or other binding instruments that apply to Google Entities or Regulated Google Cloud Customers that use or provide the Services or the Google Cloud Products (as applicable) may change over time ("Change in Law"). Upon request, You will work with Google in good faith to assess and, where necessary and mutually agreed, address the impact of a Change in Law on the Services and the Agreement.

Annex I

ICT Services

Type of ICT services	**Description**
1. ICT project management	Provision of services related to Project Management Officer (PMO)
2. ICT Development	Provision of services related to: business analysis, software design and development, testing.
3. ICT help desk and first level support	Provision of services related to: helpdesk support and first level support on ICT incident

Type of ICT services	Description
4. ICT security management services	Provision of services related to: ICT security (protection, detection, response and recovering), including security incident handling and forensics.)
5. Provision of data	Subscription to the services of data providers.
6. Data analysis	Provision of services related to the support for data analysis.
7. ICT, facilities and hosting services (excluding Cloud services)	Provision of ICT infrastructure, facilities and hosting services. This includes the provision of utilities (energy, heat management...), telecom access and physical security. (excluding Cloud services)
8. Computation	Provision of digital processing capabilities (including data computation). This excludes the computation services performed in the context of a cloud environment.
9. Non-Cloud Data storage	Provision of data storage platform (excluding Cloud services)
10. Telecom carrier	Operations for telecommunication systems and flow management. Traditional analogue telephone services are explicitly excluded as per Article 3(21) of Regulation (EU) 2022/2554
11. Network infrastructure	Provision of network infrastructure

Type of ICT services	Description
12. Hardware and physical devices	Provision of workstations, phones, servers, data storage devices, appliances, etc. in a form of a service
13. Software licencing (excluding SaaS)	Provision of software run on premises.
14. ICT operation management (including maintenance)	Provision of services related to: infrastructure (systems and hardware except network) configuration, maintenance, installing, capacity management, business continuity management, etc. Including Managed Service Providers (MSP)
15. ICT Consulting	Provision of intellectual / ICT expertise services.
16. ICT Risk management	Verification of compliance with ICT risk management requirements in accordance with Article 6(10) of Regulation (EU) 2022/2554
17. Cloud services: IaaS	Infrastructure-as-a-Service
18. Cloud services: PaaS	Platform-as-a-Service
19. Cloud services: SaaS	Software-as-a-Service

Information Protection Addendum Version 13

Last Updated September 1, 2025

Previous Versions

- Version 12 - April 10, 2025
- Version 11 - June 5, 2024
- Version 10 - September 23, 2023
- Version 9 - October 5, 2022

- Version 8 - October 27, 2021