Google Data Processing Addendum for Products Where Google is a Data Processor

Google and the counterparty agreeing to this addendum ("**Partner**") have entered into an agreement for the provision of the Processor Services (as amended from time to time, the "**Agreement**").

This Google Data Processing Addendum (including the appendices, "**Data Processing Addendum**") is entered into by Google and Partner and supplements the Agreement. This Data Processing Addendum will be effective, and replace any previously applicable terms relating to their subject matter (including any data processing amendment or data processing addendum relating to the Processor Services), from the Terms Effective Date.

If you are accepting this Data Processing Addendum on behalf of Partner, you warrant that: (a) you have full legal authority to bind Partner to this Data Processing Addendum; (b) you have read and understand this Data Processing Addendum; and (c) you agree, on behalf of Partner, to this Data Processing Addendum. If you do not have the legal authority to bind Partner, please do not accept this Data Processing Addendum.

1. Introduction

This Data Processing Addendum reflects the parties' agreement on the terms governing the processing of Partner Personal Data.

2. Definitions and Interpretation

2.1 In this Data Processing Addendum:

"**Additional Product**" means a product, service or application provided by Google or a third party that: (a) is not part of the Processor Services; and (b) is accessible for use within the user interface of the Processor Services or is otherwise integrated with the Processor Services.

"**Additional Terms**" means the additional terms referred to in Appendix 3, which reflect the parties' agreement on the terms governing the processing of Partner Personal Data in connection with certain Applicable Data Protection Legislation.

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

"**Applicable Data Protection Legislation**" means, as applicable to the processing of Partner Personal Data, any national, federal, EU, state, provincial or other privacy, data security or data protection law or regulation including European Data Protection Legislation, the LGPD and US State Privacy Laws.

"**Data Incident**" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Partner Personal Data on systems managed by or otherwise controlled by Google. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Partner Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Data Subject Tool**" means a tool (if any) made available by a Google Entity to data subjects that enables Google to respond directly and in a standardised manner to certain requests from data subjects in relation to Partner Personal Data (for example, online advertising settings or an opt-out browser plugin).

"**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**European Data Protection Legislation**" means, as applicable: (a) the GDPR; and/or (b) the Swiss FDPA.

"**GDPR**" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

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

"**Google Entity**" means Google LLC, Google Ireland Limited or any other Affiliate of Google LLC.

"**Instructions**" has the meaning given in Section 5.2 (Partner's Instructions).

"**ISO 27001 Certification**" means ISO/IEC 27001:2013 certification or a comparable certification for the Processor Services.

"**LGPD**" means the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais).

"**New Subprocessor**" has the meaning given in Section 11.1 (Consent to Subprocessor Engagement).

"**Notification Email Address**" means the email address designated by Partner, via the user interface of the Processor Services or such other means provided by Google, to receive certain notifications from Google relating to this Data Processing Addendum.

"**Partner Personal Data**" means personal data that is processed by Google on behalf of Partner in Google's provision of the Processor Services.

"**Processor Services**" means the applicable services listed at business.safety.google/services/.

"**Security Documentation**" means the certificate issued for the ISO 27001 Certification and any other security certifications or documentation that Google may make available in respect of the Processor Services.

"**Security Measures**" has the meaning given in Section 7.1.1 (Google's Security Measures).

"**Subprocessors**" means third parties authorised under this Data Processing Addendum to have logical access to and process Partner Personal Data in order to provide parts of the Processor Services and any related technical support.

"**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).

"**Term**" means the period from the Terms Effective Date until the end of Google's provision of the Processor Services under the Agreement.

"**Terms Effective Date**" means the date on which Partner clicked to accept or the parties otherwise agreed to this Data Processing Addendum.

"**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

"**US State Privacy Laws**" means US privacy, data security, and data protection laws and regulations applicable to the personal information processed by a party

under the Agreement, including without limitation: (i) the California Consumer Privacy Act of 2018 (including as amended by the California Privacy Rights Act of 2020), together with all implementing regulations ("**CCPA**"); (ii) Virginia's Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq.; and (iii) the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq. together with all implementing regulations; (iv) Connecticut's Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015; and (v) the Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.

2.2 The terms "**controller**", "**data subject**", "**personal data**", "**processing**" and "**processor**" as used in this Data Processing Addendum have the meanings given by either (a) Applicable Data Protection Legislation; or (b) absent any such meaning or law, the GDPR.

2.3 The words "**include**" and "**including**" mean "including but not limited to". Any examples in this Data Processing Addendum are illustrative and not the sole examples of a particular concept.

2.4 Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

2.5 To the extent any translated version of this Data Processing Addendum is inconsistent with the English version, the English version will govern.

3. Duration of this Data Processing Addendum

This Data Processing Addendum will take effect on the Terms Effective Date. Regardless of whether the Agreement has terminated or expired, this Data Processing Addendum will remain in effect until, and automatically expire when, Google deletes all Partner Personal Data as described in this Data Processing Addendum.

4. Application of this Data Processing Addendum

4.1 General. This Data Processing Addendum will only apply to the Processor Services for which the parties agreed to, for example: (a) the Processor Services for which Partner clicked to accept this Data Processing Addendum; or (b) if the Agreement incorporates this Data Processing Addendum by reference, the Processor Services that are the subject of the Agreement.

4.2 Incorporation of Additional Terms. The Additional Terms supplement this Data Processing Addendum.

5. Processing of Data

5.1 Roles and Regulatory Compliance; Authorisation.

5.1.1 Processor and Controller Responsibilities. The parties acknowledge and agree that:

(a) Appendix 1 describes the subject matter and details of the processing of Partner Personal Data;

(b) Google is a processor of Partner Personal Data;

(c) Partner is a controller or processor, as applicable, of Partner Personal Data; and

(d) each party will comply with the obligations applicable to it under Applicable Data Protection Legislation with respect to the processing of Partner Personal Data.

5.1.2 Processor Partners. If Partner is a processor:

(a) Partner warrants on an ongoing basis that the relevant controller has authorised: (i) the Instructions, (ii) Partner's appointment of Google as another processor, and (iii) Google's engagement of Subprocessors as described in Section 11 (Subprocessors);

(b) Partner will forward to the relevant controller promptly and without undue delay any notice provided by Google under Sections 7.2.1 (Incident Notification) or 11.4 (Opportunity to Object to Subprocessor Changes); and

(c) Partner may make available to the relevant controller any information made available by Google under Sections 7.4 (Security Certification), 10.2 (Data Centre Information) and 11.2 (Information about Subprocessors).

5.2 Partner's Instructions. By entering into this Data Processing Addendum, Partner instructs Google to process Partner Personal Data only in accordance with applicable law: (a) to provide the Processor Services and any related technical support; (b) as further specified via Partner's use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support; (c) as documented in the form of the Agreement (including this Data Processing Addendum); and (d) as further documented in any other written instructions given by Partner and acknowledged by Google as constituting instructions for purposes of this Data Processing Addendum (collectively, the "**Instructions**").

5.3 Google's Compliance with Instructions. Google will comply with the Instructions unless prohibited by applicable laws, or such applicable laws require other processing.

5.4 Additional Products. If Partner uses any Additional Product, the Processor Services may allow that Additional Product to access Partner Personal Data as required for the interoperation of the Additional Product with the Processor Services. For clarity, this Data Processing Addendum does not apply to the processing of personal data in connection with the provision of any Additional Product used by Partner, including personal data transmitted to or from that Additional Product. As necessary, the parties will enter into separate data processing terms to address how the Additional Product will process Partner Personal Data.

6. Data Deletion

6.1 Deletion During Term.

6.1.1 Processor Services With Deletion Functionality. During the Term, if:

(a) the functionality of the Processor Services includes the option for Partner to delete Partner Personal Data;

(b) Partner uses the Processor Services to delete certain Partner Personal Data; and

(c) the deleted Partner Personal Data cannot be recovered by Partner (for example, from the "trash"),

then Google will delete such Partner Personal Data from its systems as soon as reasonably practicable, unless applicable laws require storage.

6.1.2 Processor Services Without Deletion Functionality. During the Term, if the functionality of the Processor Services does not include the option for Partner to delete Partner Personal Data, then Google will comply with:

(a) any reasonable request from Partner to facilitate such deletion, insofar as this is possible taking into account the nature and functionality of the Processor Services and unless applicable laws require storage; and

(b) Google may charge a fee (based on Google's reasonable costs) for any data deletion under Section 6.1.2 (a). Google will provide Partner with

further details of any applicable fee, and the basis of its calculation, in advance of any such data deletion.

6.2 **Deletion on Term Expiry.** Partner instructs Google to delete all remaining Partner Personal Data (including existing copies) from Google's systems at the end of the Term in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable, unless applicable laws require storage.

7. Data Security

7.1 **Google's Security Measures and Assistance.**

7.1.1 **Google's Security Measures.** Google will implement and maintain technical and organisational measures to protect Partner Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Appendix 2 (the "**Security Measures**"). As described in Appendix 2, the Security Measures include measures: (a) to encrypt personal data; (b) to help ensure the ongoing confidentiality, integrity, availability and resilience of Google's systems and services; (c) to help restore timely access to personal data following an incident; and (d) for regular testing of effectiveness. Google may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

7.1.2 **Access and Compliance.** Google will: (a) authorise its employees, contractors and Subprocessors to access Partner Personal Data only as strictly necessary to comply with the Instructions; (b) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance; and (c) ensure that all persons authorised to process Partner Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3 **Google's Security Assistance.** Google will (taking into account the nature of the processing of Partner Personal Data and the information available to Google) assist Partner in ensuring compliance with Partner's (or, where Partner is a processor, the relevant controller's) obligations relating to security of personal data and personal data breaches under Applicable Data Protection Legislation, by:

(a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

(b) complying with the terms of Section 7.2 (Data Incidents); and

(c) providing Partner with the Security Documentation in accordance with Section 7.5 (Verifying Compliance) and the information contained in these Data ProcessingTerms.

7.2 **Data Incidents.**

7.2.1 **Incident Notification.** If Google becomes aware of a Data Incident, Google will: (a) notify Partner of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimise harm and secure Partner Personal Data.

7.2.2 **Details of Data Incident.** Notifications made under Section 7.2.1 (Incident Notification) will describe: the nature of the Data Incident including the Partner resources impacted; the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Google recommends that Partner take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Google's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3 **Delivery of Notification.** Google will deliver its notification of any Data Incident to the Notification Email Address or, at Google's discretion (including if Partner has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Partner is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

7.2.4 **Third Party Notifications.** Partner is solely responsible for complying with incident notification laws applicable to Partner and fulfilling any third-party notification obligations related to any Data Incident.

7.2.5 **No Acknowledgement of Fault by Google.** Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3 **Partner's Security Responsibilities and Assessment.**

7.3.1 **Partner's Security Responsibilities.** Partner agrees that, without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures and Assistance) and 7.2 (Data Incidents):

(a) Partner is responsible for its use of the Processor Services, including:

(i) making appropriate use of the Processor Services to ensure a level of security appropriate to the risk in respect of Partner Personal Data; and

(ii) securing the account authentication credentials, systems and devices Partner uses to access the Processor Services; and

(b) Google has no obligation to protect Partner Personal Data that Partner elects to store or transfer outside of Google's and its Subprocessors' systems.

7.3.2 **Partner's Security Assessment.** Partner acknowledges and agrees that the Security Measures implemented and maintained by Google as set out in Section 7.1.1 (Google's Security Measures) provide a level of security appropriate to the risk in respect of Partner Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Partner Personal Data as well as the risks to individuals.

7.4 **Security Certification.** To evaluate and help ensure the continued effectiveness of the Security Measures, Google will maintain the ISO 27001 Certification or other appropriate measures to demonstrate the effectiveness of the Security Measures.

7.5 **Verifying Compliance** To demonstrate compliance by Google with its obligations under this Data Processing Addendum, and to assist Partner in verifying Google's compliance with (i) Partner's Instructions; (ii) its obligations under this Data Processing Addendum; and (iii) its obligations under Applicable Data Protection Legislation, Google will :

(a) make the Security Documentation available for review by Partner;

(b) provide the information contained in this Data Processing Addendum; and

(c) provide or otherwise make available, in accordance with Google's standard practices, other materials concerning the nature of the Processor Services and the processing of Partner Personal Data (for example, help centre materials). Partner may also verify Google's compliance with its obligations under this Data Processing Addendum by reviewing the certificate issued for the ISO 27001 Certification (which reflects the outcome of an audit conducted by a third party auditor).

8. Impact Assessments and Consultations

Google will (taking into account the nature of the processing and the information available to Google) assist Partner in ensuring compliance with Partner's (or, where Partner is a processor, the relevant controller's) obligations relating to data protection impact assessments and prior regulatory consultations under Applicable Data Protection Legislation, by:

(a) providing the Security Documentation in accordance with Section 7.5 (Verifying Compliance);

(b) providing the information contained in the Agreement (including these Data Processing Terms); and

(c) providing or otherwise making available, in accordance with Google's standard practices, other materials concerning the nature of the Processor Services and the processing of Partner Personal Data (for example, help centre materials).

9. Data Subject Rights

9.1 **Responses to Data Subject Requests.** If Google receives a request from a data subject in relation to Partner Personal Data, Partner authorises Google to, and Google hereby notifies Partner that it will:

(a) respond directly to the data subject's request in accordance with the standard functionality of the Data Subject Tool (if the request is made via a Data Subject Tool); or

(b) advise the data subject to submit their request to Partner, and Partner will be responsible for responding to such request (if the request is not made via a Data Subject Tool).

9.2 **Google's Data Subject Request Assistance.** Google will assist Partner in fulfilling its (or, where Partner is a processor, the relevant controller's) obligations under Applicable Data Protection Legislation to respond to requests for exercising the data subject's rights, in all cases taking into account the nature of the processing of Partner Personal Data and, if applicable, Article 11 of the GDPR, by:

(a) providing the functionality of the Processor Services;

(b) complying with the commitments set out in Section 9.1 (Responses to Data Subject Requests); and

(c) if applicable to the Processor Services, making available Data Subject Tools.

9.3 **Rectification.** If Partner becomes aware that any Partner Personal Data is inaccurate or outdated, Partner will be responsible for rectifying or deleting that data if required by Applicable Data Protection Legislation, including (where available) by using the functionality of the Processor Services.

10. Data Transfers

10.1 **Data Storage and Processing Facilities.** Subject to any provisions applicable to data transfers set out in the Additional Terms, Google may process Partner Personal Data in any country in which Google or its Subprocessors maintain facilities.

10.2 **Data Centre Information.** Information about the locations of Google data centres is available at www.google.com/about/datacenters/locations/.

11. Subprocessors

11.1 **Consent to Subprocessor Engagement.** Partner specifically authorises the engagement as Subprocessors of those entities listed as of the Terms Effective Date at the URL specified in Section 11.2 (Information about Subprocessors). In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes) Partner generally authorises the engagement of any other third parties as Subprocessors ("**New Subprocessors**").

11.2 **Information about Subprocessors.** Information about Subprocessors is available at business.safety.google/subprocessors/.

11.3 **Requirements for Subprocessor Engagement.** When engaging any Subprocessor, Google will:

(a) ensure via a written contract that the Subprocessor only accesses and uses Partner Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this Data Processing Addendum); and

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

11.4 **Opportunity to Object to Subprocessor Changes.**

(a) When any New Subprocessor is engaged during the Term, Google will, at least 30 days before the New Subprocessor processes any Partner Personal Data, inform Partner of the engagement (including the name and location of the relevant New Subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

(b) Partner may object to any New Subprocessor by terminating the Agreement for convenience immediately upon written notice to Google, on condition that Partner provides such notice within 90 days of being informed of the engagement of the New Subprocessor as described in Section 11.4(a).

12. Contacting Google; Processing Records

12.1 **Contacting Google.** Partner may contact Google in relation to the exercise of its rights under this Data Processing Addendum at legal-notices@google.com or through other means as may be provided by Google.

12.2 **Google's Processing Records.** Google will keep appropriate documentation of its processing activities as required by Applicable Data Protection Legislation. Upon reasonable request, Partner will provide appropriate documentation of its processing activities to Google through the user interface of the Processor Services or by such other means as may be provided by Google, and will use such user interface or other means to ensure that all information provided is kept accurate and up-to-date.

12.3 **Controller Requests.** If Google receives a request or instruction via the methods described in Section 12.1 (or any other method) from a third party purporting to be a controller of Partner Personal Data, Google will advise the third party to contact Partner.

13. Liability

If the Agreement is governed by the laws of:

(a) a state of the United States of America, then, regardless of anything else in the Agreement, the total liability of either party towards the other party under or in connection with this Data Processing Addendum will be limited to the maximum monetary or payment-based amount at which that party's liability is capped under the Agreement (and therefore, any exclusion of indemnification claims from the Agreement's limitation of liability will not apply to indemnification claims under the Agreement relating to the Applicable Data Protection Legislation); or

(b) a jurisdiction that is not a state of the United States of America, then the total combined liability of the parties and their affiliates under or in connection with this Data Processing Addendum will be subject to the Agreement.

14. Effect of these Data Processing Terms

14.1 **Order of Precedence.** If there is any conflict or inconsistency between the Additional Terms , the remainder of this Data Processing Addendum and/or the remainder of the Agreement, then the following order of precedence will apply:

(a) the Additional Terms (if applicable);

(b) the remainder of this Data Processing Addendum; and

(c) the remainder of the Agreement.

Subject to the amendments in this Data Processing Addendum, the Agreement remains in full force and effect.

14.2 **No Effect on Controller Terms.** This Data Processing Addendum will not affect any separate terms between Google and Partner reflecting a controller-controller relationship for a service other than the Processor Services.

15. Changes to this Data Processing Addendum

15.1 **Changes to URLs.** From time to time, Google may change any URL referenced in this Data Processing Addendum and the content at any such URL, except that Google may only change the list of potential Processor Services at business.safety.google/services:

(a) to reflect a change to the name of a service;

(b) to add a new service; or

(c) to remove a service (or a feature of a service) where either: (i) all contracts for the provision of that service are terminated; (ii) Google has Partner's consent; or (iii) the service, or a certain feature of the service, has been recategorised as a controller service.

15.2 **Changes to Data Processing Addendum.** Google may change this Data Processing Addendum if the change:

(a) is expressly permitted by these Data Processing Terms, including as described in Section 15.1 (Changes to URLs);

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

(c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency, or reflects Google's adoption of a DataTransfer Solution (as defined in Appendix 3A); or

(d) does not: (i) result in a degradation of the overall security of the Processor Services; (ii) expand the scope of, or remove any restrictions on, (x) in the case of the Additional Terms, Google's rights to use or otherwise process the data in scope of the Additional Terms or (y) in the case of the remainder of this Data Processing Addendum, Google's processing of Partner Personal Data, as described in Section 5.3 (Google's Compliance with Instructions); and (iii) otherwise have a material adverse impact on Partner's rights under this Data Processing Addendum, as reasonably determined by Google.

15.3 **Notification of Changes.** If Google intends to change this Data Processing Addendum under Section 15.2(c) or (d), Google will inform Partner at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by either: (a) sending an email to the Notification Email Address; or (b) alerting Partner via the user interface for the Processor Services. If Partner objects to any such change, Partner may terminate the Agreement for convenience by giving written notice to Google within 90 days of being informed by Google of the change.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Processor Services and any related technical support to Partner.

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Partner Personal Data by Google in accordance with this Data Processing Addendum.

Nature and Purpose of the Processing

Google will process (including, as applicable to the Processor Services and the Instructions collecting, recording, organising, structuring, storing, altering, retrieving, using, disclosing, combining, erasing and destroying) Partner Personal Data for the purpose of providing the Processor Services and any related technical support to Partner in accordance with this Data Processing Addendum.

Types of Personal Data

Partner Personal Data may include the types of personal data described at business.safety.google/services.

Categories of Data Subjects

Partner Personal Data will concern the following categories of data subjects:

- data subjects about whom Google collects personal data in its provision of the Processor Services; and/or
- data subjects about whom personal data is transferred to Google in connection with the Processor Services by, at the direction of, or on behalf of Partner.

Depending on the nature of the Processor Services, these data subjects may include individuals: (a) to whom online advertising has been, or will be, directed; (b) who have visited specific websites or applications in respect of which Google provides the Processor Services; and/or (c) who are Partners or users of Partner's products or services.

Appendix 2: Security Measures

As from the Terms Effective Date, Google will implement and maintain the Security Measures set out in this Appendix 2. Google may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

1. Data Centre & Network Security

(a) **Data Centres.**

Infrastructure. Google maintains geographically distributed data centres. Google stores all production data in physically secure data centres.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimise the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Processor Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data centre equipment is scheduled through a standard process according to documented procedures.

Power. The data centre electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data centre. Backup power is provided by various mechanisms such as uninterruptible power supply (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data centre, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data centre at full capacity typically for a period of days.

Server Operating Systems. Google servers use hardened operating systems which are customised for the unique server needs of the business. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Processor Services and enhance the security products in production environments.

Business Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

Encryption Technologies. Google's security policies mandate encryption at rest for all user data, including personal data. Data is often encrypted at multiple levels in Google's production storage stack in data centres, including at the hardware level, without requiring any action by partners. Using multiple layers of encryption adds redundant data protection and allows Google to select the optimal approach based on application requirements. All personal data is encrypted at the storage level, generally using AES256. Google uses common cryptographic libraries which incorporate Google's FIPS 140-2 validated module, to implement encryption consistently across the Processor Services.

(b) **Networks & Transmission**.

Data Transmission. Data centres are typically connected via high-speed private links to provide secure and fast data transfer between data centres. Further, Google encrypts data transmitted between data centres. This is designed to prevent data from being read, copied, altered or removed without authorisation during electronic transport. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. Employing intelligent detection controls at data entry points; and
3. Employing technologies that automatically remedy certain dangerous situations.

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

Encryption Technologies. Google makes HTTPS encryption (also referred to as TLS connection) available. Google servers support ephemeral elliptic curve Diffie Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimise the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls

(a) **Site Controls**.

On-site Data Centre Security Operation. Google's data centres maintain an on-site security operation responsible for all physical data centre security functions 24 hours a day, 7 days a week. The on-site security operations personnel monitor Closed Circuit TV ("**CCTV**") cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data centre regularly.

Data Centre Access Procedures. Google maintains formal access procedures for allowing physical access to the data centres. The data centres are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data centre are required to identify themselves as well as show proof of identity to on-site security operations. Only authorised employees, contractors and visitors are allowed entry to the data centres. Only authorised employees and contractors are permitted to request electronic card key access to these facilities. Data centre electronic card key access requests must be made in advance and in writing, and require the approval of authorised data centre personnel. All other entrants requiring temporary data centre access must: (i) obtain approval in advance from authorised data centre personnel for the specific data centre and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data centre access record identifying the individual as approved.

On-site Data Centre Security Devices. Google's data centres employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorised activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorised access throughout the business operations and data centres is restricted based on zones and the individual's job responsibilities. The fire doors at the data centres are alarmed. CCTV cameras are in operation both inside and outside the data centres. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data centre building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centres connect the CCTV equipment. Cameras record on-site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for at least 7 days based on activity.

(b) **Access Control**.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Processor Services, and responding to security incidents.

Access Control and Privilege Management. Partner's administrators and users must authenticate themselves via a central authentication system or via a single sign-on system in order to use the Processor Services.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorised persons to

access data they are authorised to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralised access management system to control personnel access to production servers, and only provides access to a limited number of authorised personnel. LDAP, Kerberos and a proprietary system utilising digital certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimise the potential for unauthorised account use. The granting or modification of access rights is based on: the authorised personnel's job responsibilities; job duty requirements necessary to perform authorised tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.

3. Data

(a) **Data Storage, Isolation & Authentication**.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Processor Services database and file system architecture are replicated between multiple geographically dispersed data centres. Google logically isolates each partner's data. A central authentication system is used across all Processor Services to increase uniform security of data.

(b) **Decommissioned Disks and Disk Destruction Guidelines**.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("**Decommissioned Disk**"). Every Decommissioned Disk is subject to a series of data destruction processes (the "**Data Destruction Guidelines**") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Data Destruction Guidelines.

(c) **Pseudonymous Data**. Online advertising data are commonly associated with online identifiers which on their own are considered 'pseudonymous' (i.e. they cannot be attributed to a specific individual without the use of additional information). Google has a robust set of policies and technical and organisational controls in place to ensure the separation between pseudonymous data and personally identifiable user information (i.e. information that could be used on its own to directly identify, contact, or precisely locate an individual), such as a user's Google account data. Google policies only allow for information flows between pseudonymous and personally identifiable data in strictly limited circumstances.

(d) **Launch reviews**. Google conducts launch reviews for new products and features prior to launch. This includes a privacy review conducted by specially trained privacy engineers. In privacy reviews, privacy engineers ensure that all applicable Google policies and guidelines are followed, including but not limited to policies relating to pseudonymisation and data retention and deletion.

4. Personnel Security

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Partner Personal Data are required to complete additional requirements appropriate to their role. Google's personnel will not process Partner Personal Data without authorisation.

5. Subprocessor Security

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms, subject to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement).

Appendix 3: Additional Terms for Applicable Data Protection Legislation

PART A - ADDITIONAL TERMS FOR EUROPEAN DATA PROTECTION LEGISLATION

1. Introduction

This Appendix 3A will only apply to the extent that the European Data Protection Legislation applies to the processing of Partner Personal Data.

2. Additional Definitions

2.1 In this Appendix 3A:

"**Adequate Country**" means:

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

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

(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 protection by the Swiss Federal Council under the Swiss FDPA,

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

"**Data Transfer Solution**" means a solution that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Legislation, including the EU-US Data Privacy Framework, UK Extension to EU-US Data Privacy Framework, Swiss-US Data Privacy Framework (collectively, the "Data Privacy Framework"), or another valid data protection framework recognized as providing adequate protection under Applicable Data Protection Legislation.

"**EEA**" means the European Economic Area.

"**European Laws**" means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Partner Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Partner Personal Data); and (c) the law of Switzerland (if the Swiss FDPA applies to the processing of Partner Personal Data).

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

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

"**SCCs (Controller-to-Processor)**" means the terms at business.safety.google/gdprcontrollerterms/sccs/eu-c2p-dpa.

"**SCCs (Processor-to-Controller)**" means the terms at business.safety.google/gdprprocessorterms/sccs/p2c.

"**SCCs (Processor-to-Processor)**" means the terms at business.safety.google/gdprprocessorterms/sccs/eu-p2p-dpa.

"**SCCs (Processor-to-Processor, Google Exporter)**" means the terms at business.safety.google/gdprprocessorterms/sccs/eu-p2p-intra-group.

"**Supervisory Authority**" means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR and/or the Swiss FDPA.

2.2 The terms "**data importer**" and "**data exporter**" have the meanings given in the applicable SCCs.

3. **Processor Partners.** If Partner is a processor, Partner will forward to the relevant controller promptly and without undue delay, any notice that refers to any SCCs.

4. **European Laws.** Where European Data Protection Legislation applies to Google's processing of Partner Personal Data, references to "applicable laws" in Sections 5.3 (Google's Compliance with Instructions), 6.1.1 (Processor Services with Deletion Functionality), 6.1.2(a) (Processor Services without Deletion Functionality) and Section 6.2 (Deletion on Term Expiry), means "European Laws."

5. **Instruction Notifications.** Google will immediately notify Partner if, in Google's opinion: (a) European Laws prohibit Google from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Legislation; or (c) Google is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law. If Partner is a processor, Partner will immediately forward to the relevant controller any notice provided by Google under this paragraph. This paragraph 5 (Instruction Notifications) does not reduce either party's rights and obligations elsewhere in the Agreement.

6. **Audits of Compliance**

6.1 **Partner's Audit Rights**.

(a) Google will allow Partner or a third party auditor appointed by Partner to conduct audits (including inspections) to verify Google's compliance with its obligations under this Data Processing Addendum in accordance with paragraph 6.2 (Additional Business Terms for Audits) of this Appendix 3A. During an audit, Google will make available all information necessary to demonstrate such compliance and contribute to the audits as described in Section 7.4 (Security Certification) and paragraph 6 (Audits of Compliance) of this Appendix 3A.

(b) If the SCCs apply under paragraph 7.1 (Restricted European Transfers) of this Appendix 3A, Google will allow Partner (or a third-party auditor appointed by Partner) to conduct audits as described in the SCCs and, during the audit, make available all information required by the SCCs, each in accordance with paragraph 6.2 (Additional Business Terms for Audits) of this Appendix 3A.

6.2 **Additional Business Terms for Audits**.

(a) Partner will send any request for an audit under paragraph 6.1(a) or 6.1(b) of this Appendix 3A to Google as described in Section 12.1 (Contacting Google).

(b) Following receipt by Google of a request under paragraph 6.2(a) of this Appendix 3A, Google and Partner will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any audit under paragraphs 6.1(a) or 6.1(b) of this Appendix 3A.

(c) Google may charge a fee (based on Google's reasonable costs) for any audit under paragraphs 6.1(a) or 6.1(b) of this Appendix 3A. Google will provide Partner with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Partner will be responsible for any fees charged by any third party auditor appointed by Partner to execute any such audit.

(d) Google may object to any third party auditor appointed by Partner to conduct any audit under paragraph 6.1(a) or 6.1(b) of this Appendix 3A if the auditor is, in Google's reasonable opinion, not suitably qualified or independent, a competitor of Google or otherwise manifestly unsuitable. Any such objection by Google will require Partner to appoint another auditor or conduct the audit itself.

(e) Nothing in these Data Processing Terms will require Google either to disclose to Partner or its third party auditor, or to allow Partner or its third party auditor to access: (i) any data of any other partner of a Google Entity; (ii) any Google Entity's internal accounting or financial information; (iii) any trade secret of a Google Entity; (iv) any information that, in Google's reasonable opinion, could: (A) compromise the security of any Google Entity's systems or premises; or (B) cause any Google Entity to breach its obligations under the European Data Protection Legislation or its security and/or privacy obligations to Partner or any third party; or (v) any information that Partner or its third party auditor seeks to access for any reason other than the good faith fulfilment of Partner's obligations under the European Data Protection Legislation.

7. **Data Transfers**

7.1 **Restricted European Transfers**. The parties acknowledge that European Data Protection Legislation does not require SCCs or a Data Transfer Solution to transfer Partner Personal Data to an Adequate Country. If Partner Personal Data is transferred to any other country, and European Data Protection Legislation applies to the transfers ("**Restricted European Transfers**"), then:

(a) The parties acknowledge that Google has adopted a DataTransfer Solution for any Restricted European Transfer, and the parties will ensure that such Restricted European Transfer is made in accordance with that solution; and/or

(b) if a Data Transfer Solution is not available, then:

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

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

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

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

7.2 **Supplementary Measures and Information**. Google will provide Partner with information relevant to Restricted European Transfers, including information about supplementary measures to protect Partner Personal Data, as described in Section 7.5 (Verifying Compliance), Appendix 2 (Security Measures) and other materials concerning the nature of the Processor Services and the processing of Partner Personal Data (for example, help centre articles).

7.3 **Termination**. If Partner concludes, based on its current or intended use of the Processor Services, that the Data Transfer Solution and/or SCCs, as applicable, do not provide appropriate safeguards for Partner Personal Data, then Partner may immediately terminate the Agreement for convenience by notifying Google in writing.

7.4 **Data Transfer Solution Adoption and Certification**. Information about Google and/or its Affiliates' adoption of, or certification under, a Data Transfer Solution can be found at https://policies.google.com/privacy/frameworks. The parties acknowledge that Google has certified under the Data Privacy Framework on behalf of

itself and certain wholly-owned US subsidiaries. Google's certification is available at https://www.dataprivacyframework.gov. The Data Privacy Framework will apply to any Restricted European Transfer to a certified Google entity in the US.

8. **Subprocessors**. When engaging any Subprocessor, Google will ensure via a written contract that if the processing of Partner Personal Data is subject to European Data Protection Legislation, the data protection obligations in these Data Processing Terms (as referred to in Article 28(3) of the GDPR, if applicable) are imposed on the Subprocessor.

9. **Google's Processing Records.**

Partner acknowledges that Google is required under the GDPR to:

(a) collect and maintain records of certain information, including: (i) the name and contact details of each processor and/or controller on behalf of which Google is acting and (if applicable) of such processor's or controller's local representative and data protection officer, and (ii) if applicable under the Partner SCCs, Partner's Supervisory Authority; and

(b) make such information available to any Supervisory Authority. Accordingly, Partner will, where requested and as applicable to Partner, provide such information to Google via the user interface of the Processor Services or via such other means as may be provided by Google, and will use such user interface or other means to ensure that all information provided is kept accurate and up-to-date.

10. **SCCs**

10.1 **Order of Precedence**. If there is any conflict or inconsistency between the Partner SCCs and this Appendix 3A, the remainder of this Data Processing Addendum or the remainder of the Agreement, then the Partner SCCs will prevail.

10.2 **No Modification of SCCs**. Nothing in the Agreement (including these Data Processing Terms) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under the European Data Protection Legislation.

11. **Changes to SCCs**. Google may only change the SCCs in accordance with Sections 15.2(b) - 15.2(d) (Changes to Data Processing Terms) or to incorporate any new version of the SCCs that may be adopted under the European Data Protection Legislation, in each case in a manner that does not affect the validity of the SCCs under the European Data Protection Legislation.

PART B - ADDITIONAL TERMS FOR US STATE PRIVACY LAWS

1. **Introduction**

Google and Partner have entered into the Google Data Processing Addendum for Products Where Google is a Data Processor ("DPA") which supplements the Agreement. This Appendix 3B reflects the parties' agreement on the processing of Partner Personal Data and Deidentified Data (as defined below) pursuant to the Agreement in connection with the US State Privacy Laws, and is effective solely to the extent each US State Privacy Law applies.

2. **Additional Definitions and Interpretation**

In this Appendix 3B:

(a) "**Deidentified Data**" means data information that is "deidentified" (as that term is defined by the CCPA) and "de-identified data" (as defined by other US State Privacy Laws), when disclosed by one party to the other.

(b) the terms "**business**", "**consumer**", "**personal information**", "**sale(s)**", "**sell**", "**service provider**", and "**share**" as used in this Appendix 3B have the meanings given in the applicable US State Privacy Laws.

3. **Applicable State Privacy Law Terms.**

3.1 To the extent that one or more of the US State Privacy Laws applies to the processing of Partner Personal Data:

3.1.1 **Roles and Regulatory Compliance; Authorization.**

(a) **Processor and Controller Responsibilities.** The parties acknowledge and agree that:

(i) Appendix 1 of these Data Processing Terms describes the subject matter and details of the processing of Partner Personal Data, subject to the following modification:

(1) The "Types of Personal Data" section is amended to include the following language: "Partner Personal Data also may include the types of personal data described under the US State Privacy Laws."

(ii) Google is a service provider and processor of Partner Personal Data under the US State Privacy Laws;

(iii) Partner is a controller or processor, as applicable, of Partner Personal Data under the US State Privacy Laws; and

(iv) Each party will comply with the obligations applicable to it under US State Privacy Laws with respect to the processing of Partner Personal Data.

(b) **Processor Partners.** If Partner is a processor:

(i) Partner warrants on an ongoing basis that the relevant controller has authorized: (A) the Instructions, (B) Partner's appointment of Google as another processor, and (C) Google's engagement of subcontractors as described in Section 11 (Subprocessors) of this Data Processing Addendum and paragraph 3.4 (Subcontractors) of this Appendix 3B.

(ii) Partner will immediately forward to the relevant controller any notice provided by Google under Section 7.2.1 (Incident Notification) and Section 11 (Subprocessors) of this Data Protection Addendum, and paragraph 3.2 (Instruction Notifications) and paragraph 3.4 (Subcontractors) of this Appendix 3B.

(iii) Partner may make available to the relevant controller any information made available by Google.

3.2 **Instruction Notifications.** Google will immediately notify Partner if, in Google's opinion: (a) US State Privacy Laws prohibit Google from complying with an Instruction; (b) an Instruction does not comply with US State Privacy Laws; or (c) Google is otherwise unable to comply with an Instruction or US State Privacy Laws, in each case unless such notice is prohibited by US State Privacy Laws. This paragraph 3.2 of this Appendix 3B (Instruction Notifications) does not reduce either party's rights and obligations elsewhere in the Agreement.

3.3 **Partner's Audit Rights.**

(i) Partner may conduct an audit to verify Google's compliance with its obligations under this Appendix 3B by requesting and reviewing (1) a certificate issued for security verification reflecting the outcome of an audit conducted by a third party auditor (e.g., SOC 2 Type II or ISO/IEC 27001 certification or a comparable certification or other security certification of an audit conducted by a third-party auditor agreed by Partner and Google) and (2) any other information Google determines is reasonably necessary for Partner to verify such compliance.

(ii) Alternatively, Google may, at its sole discretion and in response to a request by Partner, initiate a third-party audit to verify Google's compliance with its obligations under this Appendix 3B. During such an audit, Google will make available to the third-party auditor all information necessary to demonstrate such compliance. Following receipt of such request, Google and Partner will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to any audit under this paragraph 3.3(ii). Where Partner requests such an audit, Google may charge a fee (based on Google's reasonable costs) for any audit. Google will provide Partner with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Partner will be responsible for any fees charged by any third-party auditor appointed by Partner to execute any such audit.

(iii) Nothing in this Appendix 3B will require Google either to disclose to Partner or its third-party auditor, or to allow Partner or its third-party auditor to access:

(1) any data of any other Partner of a Google Entity;

(2) any Google Entity's internal accounting or financial information;

(3) any trade secret of a Google Entity;

(4) any information that, in Google's reasonable opinion, could: (A) compromise the security of any Google Entity's systems or premises; or (B) cause any Google Entity to breach its obligations under the US State Privacy Laws or its security and/or privacy obligations to Partner or any third party; or

(5) any information that Partner or its third party auditor seeks to access for any reason other than the good faith fulfillment of Partner's obligations under the US State Privacy Laws.

3.4 **Subcontractors.** When engaging any Subprocessor, Google will ensure via a written contract that

(i) if the processing of Partner Personal Data is subject to the US State Privacy Laws, the data protection obligations in this Data Processing Addendum, including this Appendix 3B, are imposed on the subcontractor.;

4. US State Privacy Law Terms

4.1 **Deidentified Data.** To the extent that one or more of the US State Privacy Laws applies to the processing of Partner Personal Data, each party will comply with the requirements for processing Deidentified Data set out in the US State Privacy Laws, with respect to any Deidentified Data it receives from the other party pursuant to the Agreement. For purposes of this paragraph 4.1 (Deidentified Data), Partner Personal Data means any personal data that is processed by a party under the Agreement in connection with its provision or use of the Processor Services.

5. Google's CCPA Obligations.

5.1 To the extent that CCPA applies to such processing of Partner Personal Data, Google will act as Partner's service provider, and as such, unless otherwise permitted for service providers under CCPA, as reasonably determined by Google:

(a) Google will not sell or share any Partner Personal Data that it obtains from Partner in connection with the Agreement;

(b) Google will not retain, use or disclose Partner Personal Data (including outside of the direct business relationship between Google and Partner), other than for a business purpose under the CCPA on behalf of Partner;

(c) Google will not combine Partner Personal Data that Google receives from, or on behalf of, Partner with (i) personal information that Google receives from, or on behalf of, another person or persons or (ii) personal information collected from Google's own interaction with a consumer, except to the extent permitted under CCPA;

(d) Google will process such Partner Personal Data for the specific purpose of performing the Processor Services, as further described in the Agreement and supporting documentation (e.g., help center articles), or as otherwise permitted under the CCPA, and the parties agree that Partner is making such Partner Personal Data available to Google for such purposes;

(e) Google will allow audits to verify Google's compliance with its obligations under this Appendix 3B in accordance with paragraph 3.3) (Partner's Audit Rights) of this Appendix 3B;

(f) Google will notify Partner if Google makes a determination that it can no longer meet its obligations under the CCPA. This paragraph 5.1(f) does not reduce either party's rights and obligations elsewhere in the Agreement;

(g) If Partner reasonably believes that Google is processing Partner Personal Data in an unauthorized manner, Partner has the right to notify Google of such belief via the methods described at legal-notices@google.com and the parties will work together in good faith to remediate the allegedly violative processing activities, if necessary; and

(h) Google will comply with applicable obligations under CCPA and will provide the same level of privacy protection as is required by CCPA.

In addition to Section 15 of the Data Processing Terms (Changes to this Data Processing Addendum), Google may change this Appendix 3B without notice if the change (a) is based on applicable law, applicable regulation, a court order, or guidance issued by a governmental regulator or agency or (b) does not have a material adverse impact on Partner under the US State Privacy Laws, as reasonably determined by Google.

Google Data Processing Addendum, Version 7.0

06 October 2023

Previous Versions

- 23 January 2023
- 22 September 2022
- 27 September 2021
- 27 August 2020
- 31 October 2019
- 4 May 2018