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 and security of certain data in connection with the European Data Protection Legislation and Non-European Data Protection Legislation.

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 for Non-European Data Protection Legislation**" means the additional terms referred to in Appendix 3, which reflect the parties' agreement on the terms governing the processing of certain data in connection with certain Non-European Data Protection Legislation.

"**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;

(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; 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 an adequate level of 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.

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

"**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).

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

"**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.

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

"**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 (formerly known as Google Inc.), Google Ireland Limited, or any other entity that directly or indirectly controls, is controlled by, or is under common control with, 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.

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

"**Non-European Data Protection Legislation**" means data protection or privacy laws in force outside the EEA, Switzerland, and the UK.

"**Notification Email Address**" means the email address (if any) designated by Partner, through 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.

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

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

"**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.

"**Security Documentation**" means the ISO 27001 Certification and any other security certifications or documentation that Google may make available in connection with 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.

"**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.

"**Swiss FDPA**" means the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**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, as applicable:

(a) 25 May 2018, if Partner clicked to accept or the parties otherwise agreed to this Data Processing Addendum before or on such date; or

(b) the date on which Partner clicked to accept or the parties otherwise agreed to this Data Processing Addendum, if such date is after 25 May 2018.

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

2.2 The terms "**controller**", "**data subject**", "**personal data**", "**processing**", and "**processor**" as used in this Data Processing Addendum have the meanings given in the GDPR, and the terms "**data importer**" and "**data exporter**" have the meanings given in the applicable SCCs.

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 and, regardless of whether the Term has expired, 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 Application of European Data Protection Legislation. Sections 5 (Processing of Data) to 12 (Contacting Google; Processing Records) (inclusive) will only apply to the extent that the European Data Protection Legislation applies to the processing of Partner Personal Data, including if:

(a) the processing is in the context of the activities of an establishment of Partner in the EEA or the UK; and/or

(b) Partner Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services or the monitoring of their behaviour in the EEA or the UK.

4.2 Application to Processor Services. This Data Processing Addendum will only apply to the Processor Services for which the parties agreed to this Data Processing Addendum (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).

4.3 Incorporation of Additional Terms for Non-European Data Protection Legislation. The Additional Terms for Non-European Data Protection Legislation 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 under the European Data Protection Legislation;

(c) Partner is a controller or processor, as applicable, of Partner Personal Data under the European Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the European 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 immediately forward to the relevant controller any notice provided by Google under Sections 5.4 (Instruction Notifications), 7.2.1 (Incident Notification), 11.4 (Opportunity to Object to Subprocessor Changes), or that refers to any SCCs; and

(c) Partner may make available to the relevant controller any information made available by Google under Sections 7.4 (Security Certification), 10.6 (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 through 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 European Laws.

5.4 **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. This Section 5.4 (Instruction Notifications) does not reduce either party's rights and obligations elsewhere in the Agreement.

5.5 **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. 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 European 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 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 European Laws require storage. Google may charge a fee (based on Google's reasonable costs) for any data deletion under this Section 6.1.2 (Processor Services Without Deletion Functionality). 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 When the Term Expires.** When the Term expires, Partner instructs Google to delete all Partner Personal Data (including existing copies) from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable unless European 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.** Taking into account the nature of the processing of Partner Personal Data and the information available to Google, Google will assist Partner in ensuring compliance with Partner's (or, where Partner is a processor, the relevant controller's) obligations regarding security of personal data and personal data breaches, including Partner's (or, where Partner is a processor, the relevant controller's) obligations under Articles 32 to 34 (inclusive) of the GDPR, 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 7.5.1 (Reviews of Security Documentation) and the information contained in this Data Processing Addendum.

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 to 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 the Security Measures implemented and maintained by Google as described in Section 7.1.1 (Google's Security Measures) provide a level of security appropriate to the risk to Partner Personal Data taking into account the nature, scope, context, and purposes of the processing of Partner Personal Data; the state of the art; the costs of implementation; and 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 Reviews and Audits of Compliance.

7.5.1 Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Data Processing Addendum, Google will make the Security Documentation available for review by Partner.

7.5.2 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 Section 7.5.3 (Additional Business Terms for Audits). During audits, 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 this Section 7.5 (Reviews and Audits of Compliance).

(b) If the SCCs apply under Section 10.2 (Restricted European Transfers), Google will allow Partner (or a third-party auditor appointed by Partner) to conduct audits as described in the applicable SCCs and, during such audits, make available all information required by those SCCs, each in accordance with Section 7.5.3 (Additional Business Terms for Audits).

(c) Partner may also conduct an audit to verify Google's compliance with its obligations under this Data Processing Addendum by reviewing any certificate(s) issued to Google by any third-party auditor(s) (for example, an ISO 27001 Certification, if any).

7.5.3 Additional Business Terms for Audits.

(a) Partner will send any request for an audit under Sections 7.5.2(a) or 7.5.2(b) to Google as described in Section 12.1 (Contacting Google).

(b) Following receipt by Google of a request under Section 7.5.3(a), 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 Section 7.5.2(a) or 7.5.2(b).

(c) Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) or 7.5.2(b). 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 Section 7.5.2(a) or 7.5.2(b) 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 this Data Processing Addendum 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 or customer 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 fulfillment of Partner's obligations under the European Data Protection Legislation.

8. Impact Assessments and Consultations

Taking into account the nature of the processing and the information available to Google, Google will assist Partner in ensuring compliance with Partner's (or where Partner is a processor, the relevant controller's) obligations regarding data protection impact assessments and prior consultation, including (if applicable) Partner's or the relevant controller's obligations under Articles 35 and 36 of the GDPR, by:

(a) providing the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation);

(b) providing the information contained in this Data Processing Addendum; 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 through 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 through a Data Subject Tool).

9.2 **Google's Data Subject Request Assistance.** Google will assist Partner (or, where Partner is a processor, the relevant controller) in fulfilling its obligations under the GDPR 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, including (if applicable):

(a) providing the functionality of the Processor Services;

(b) complying with the commitments 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 the European 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 the remainder of this Section 10 (Data Transfers), Google may process Partner Personal Data in any country in which Google or any of its Subprocessors maintains facilities.

10.2 **Restricted European Transfers.** The parties acknowledge that the European Data Protection Legislation does not require the SCCs or an Alternative Transfer Solution in order to process Partner Personal Data in or transfer it to an Adequate Country.

If Partner Personal Data is transferred to any other country, and the European Data Protection Legislation applies to those transfers ("**Restricted European Transfer**"), then:

(a) if Google adopts an Alternative Transfer Solution for any Restricted European Transfers, then Google will inform Partner of the relevant solution and ensure that such Restricted European Transfers are made in accordance with that solution; and/or

(b) if Google has not adopted, or has informed Partner that Google is no longer adopting an Alternative Transfer Solution for any Restricted European Transfers, 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

10.3 **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 7.5.1 (Reviews of Security Documentation), 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).

10.4 **Termination.** If Partner concludes, based on its current or intended use of the Processor Services, that the Alternative 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.

10.5 **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 of the Subprocessors listed in Section 11.2 (Information about Subprocessors) as of the Terms Effective Date. In addition, Partner generally authorises the engagement of any other third parties as Subprocessors ("**New Subprocessors**"), subject to Section 11.4 (Opportunity to Object to Subprocessor Changes).

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 through a written contract that:

(i) 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

(ii) if the processing of Partner Personal Data is subject to the European Data Protection Legislation, the data protection obligations in this Data Processing Addendum (as referred to in Article 28(3) of the GDPR, if applicable) are imposed on the Subprocessor; 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) If any New Subprocessor is engaged during the Term, then at least 30 days before the New Subprocessor processes any Partner Personal Data, Google will inform Partner of the engagement (including the name and location of the relevant 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. When exercising its rights under this Data Processing Addendum, Partner may contact Google at legal-notices@google.com or through such 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 the GDPR. 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 relevant SCCs, Partner's Supervisory Authority; and (b) make such information available to any Supervisory Authority. Accordingly, where requested and as applicable Partner will provide such information 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 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 confidentiality or indemnification claims from the Agreement's limitation of liability will not apply to claims under the Agreement relating to the European Data Protection Legislation or the Non-European Data Protection Legislation); or

(b) a jurisdiction that is not a state of the United States, 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 this Data Processing Addendum

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

(a) the SCCs;

(b) the Additional Terms for Non-European Data Protection Legislation;

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

(d) 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 Modification of SCCs.** Nothing in the Agreement (including this Data Processing Addendum) is intended to modify or contradict any SCCs or reduce the fundamental rights or freedoms of data subjects under the European Data Protection Legislation.

14.3 **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.

14.4 **Legacy UK SCCs.** As of 21 September 2022 or the Agreement's effective date, whichever is later, the SCCs' supplementary terms for UK GDPR transfer will apply, and will supersede and terminate any standard contractual clauses approved under the UK GDPR and the Data Protection Act 2018 and previously entered into by Partner and Google (" **Legacy UK SCCs** "). This Section 14.4 (Legacy UK SCCs) will not affect either party's rights, or any data subject's rights, that may have accrued under the Legacy UK SCCs while they were in force.

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:

(a) the SCCs in accordance with Sections 15.2(b) - 15.2(d) (Changes to Data Processing Addendum) 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 SCC under the European Data Protection Legislation; and

(b) the list of potential Processor Services at business.safety.google/services:

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

(ii) to add a new service (or a feature of a service); or

(iii) to remove a service (or a feature of a service) where either: (x) all contracts for the provision of that service are terminated; (y) Google has Partner's consent; or (z) the service (or a 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 this Data Processing Addendum, 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 an Alternative Transfer Solution; 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 for Non-European Data Protection Legislation, Google's rights to use or otherwise process the data in scope of the Additional Terms for Non-European Data Protection Legislation 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 through 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 Partner Personal Data, including (as applicable to the nature of 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:

- individuals to whom online advertising has been, or will be, directed;
- 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 connection with the Processor Services; and/or (c) who are customers 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 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 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 or customers. 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. 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 on-site security operations 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 operations 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 the authorised data centre personnel. All other entrants requiring temporary data centre access must: (i) obtain approval in advance from the data centre managers 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 using a central authentication system or 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 (for example, 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 and 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 or customer'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 Subprocessors' security and privacy practices 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 in Section 11.3 (Requirements for

Subprocessor Engagement).

Appendix 3: Additional Terms for Non-European Data Protection Legislation

The following Additional Terms for Non-European Data Protection Legislation supplement this Data Processing Addendum:

- CCPA Service Provider Addendum at business.safety.google/processorterms/ccpa (dated 27 August 2020)
- LGPD Processor Addendum at business.safety.google/processorterms/lgpd (dated 27 August 2020)
- U.S. State Law Addendum at business.safety.google/processorterms/us-state-laws (effective 1 January 2023 replacing the CCPA Service Provider Addendum)

Google Data Processing Addendum, Version 4.0

22 September 2022

Previous Versions

- 27 September 2021
- 27 August 2020
- 31 October 2019
- 4 May 2018