Google

Privacy Policy

Business Data Responsibility

Google Ads Data Processing Terms

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

These Google Ads Data Processing Terms (including the appendices, "**Data Processing Terms**") are entered into by Google and Customer and supplement the Agreement. These Data Processing Terms 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 these Data Processing Terms on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to these Data Processing Terms; (b) you have read and understand these Data Processing Terms; and (c) you

These Data Processing Terms reflect the parties' agreement on the terms governing the processing of Customer Personal Data.

2. Definitions and Interpretation

2.1 In these Data Processing Terms:

"**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 Customer 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 Customer 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.

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

"**Data Incident**" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer 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 Customer Personal Data, including unsuccessful log-in

certain requests from data subjects in relation to Customer 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 (Customer'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 Customer, via the user interface of the Processor Services or such other means provided by Google, to receive certain notifications from Google relating to these Data Processing Terms.

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

Measures).

"**Subprocessors**" means third parties authorised under these Data Processing Terms to have logical access to and process Customer 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 Customer clicked to accept or the parties otherwise agreed to these Data Processing Terms.

"**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**" has the meaning found at business.safety.google/usdataprotectionlaws.

2.2 The terms "**controller**", "**data subject**", "**personal data**", "**processing**" and "**processor**" as used in these Data Processing Terms 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 these Data Processing Terms 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.

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

4. Application of these Data Processing Terms

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

4.2 **Incorporation of Additional Terms**. The Additional Terms supplement these Data Processing Terms.

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 Customer Personal Data;

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

Google

Privacy Policy

Business Data Responsibility

5.1.2 **Processor Customers**. If Customer is a processor:

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

(b) Customer 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) Customer 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 **Customer's Instructions**. By entering into these Data Processing Terms, Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Processor Services and any related technical support; (b) as further specified via Customer'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 these Data Processing Terms); and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of these Data Processing Terms (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 Customer uses any Additional Product, the Processor Services may allow that Additional Product to access Customer Personal Data as required for the interoperation of the Additional Product with the Processor Services. For clarity, these Data Processing Terms do not apply to the processing of personal data in connection with the provision of any Additional Product used by Customer,

Google

Privacy Policy

Business Data Responsibility

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 Customer to delete Customer Personal Data;

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

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

then Google will delete such Customer Personal Data from its systems as soon as reasonably practicable and within a maximum period of 180 days, 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 Customer to delete Customer Personal Data, then Google will comply with:

(a) any reasonable request from Customer 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) the data retention practices described at policies.google.com/technologies/ads.

Google may charge a fee (based on Google's reasonable costs) for any data deletion under Section 6.1.2(a). Google will provide Customer 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**. Customer instructs Google to delete all remaining Customer 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 and within a maximum period of 180

Google

Privacy Policy

Business Data Responsibility

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 Customer 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 Customer 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 Customer 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 Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with Customer's (or, where Customer 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 Customer with the Security Documentation in accordance with Section 7.5 (Verifying Compliance) and the information contained in these Data Processing Terms.

(b) promptly take reasonable steps to minimise harm and secure Customer 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 Customer 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 Customer 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 Customer has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Customer 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**. Customer is solely responsible for complying with incident notification laws applicable to Customer 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 **Customer's Security Responsibilities and Assessment**.

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

uses to access the Processor Services; and

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

7.3.2 **Customer's Security Assessment**. Customer 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 Customer 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 Customer 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.

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

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

(b) provide the information contained in the Data Processing Terms; 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 Customer Personal Data (for example, help centre materials). Customer may also verify Google's compliance with its obligations under these Data Processing Terms 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

(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 Customer 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 Customer Personal Data, Customer authorises Google to, and Google hereby notifies Customer 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 Customer, and Customer 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 Customer in fulfilling its (or, where Customer 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 Customer 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

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 Customer 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**. Customer 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) Customer 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/adssubprocessors.

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 Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Data Processing Terms); and

days before the New Subprocessor processes any Customer Personal Data, inform Customer 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) Customer may object to any New Subprocessor by terminating the Agreement for convenience immediately upon written notice to Google, on condition that Customer 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**. Customer may contact Google in relation to the exercise of its rights under these Data Processing Terms via the methods described at privacy.google.com/businesses/processorsupport or via such other means as may be provided by Google from time to time. Google will provide prompt and reasonable assistance with Customer queries Google receives via such means, and that relate to the processing of Customer Personal Data under the Agreement.

12.2 **Google's Processing Records**. Google will keep appropriate documentation of its processing activities as required by Applicable Data Protection Legislation.

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 Customer Personal Data, Google will advise the third party to contact Customer.

13. Liability

If the Agreement is governed by the laws of:

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 liability of the parties under or in connection with these Data Processing Terms will be subject to the exclusions and limitations of liability in 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 these Data Processing Terms 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 these Data Processing Terms; and

(c) the remainder of the Agreement.

Subject to the amendments in these Data Processing Terms, the Agreement remains in full force and effect.

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

15. Changes to these Data Processing Terms

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

provision of that service are terminated; (ii) Google has Customer'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 Terms.** Google may change these Data Processing Terms 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 an Alternative Transfer 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 these Data Processing Terms, Google's processing of Customer Personal Data, as described in Section 5.3 (Google's Compliance with Instructions); and (iii) otherwise have a material adverse impact on Customer's rights under these Data Processing Terms, as reasonably determined by Google.

15.3 **Notification of Changes**. If Google intends to change these Data Processing Terms under Section 15.2(c) or (d), Google will inform Customer 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 Customer via the user interface for the Processor Services. If Customer objects to any such change, Customer may immediately terminate the Agreement for convenience by giving written notice to Google within 90 days of being informed by Google of the change.

Google

Privacy Policy

Business Data Responsibility

Subject Matter

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

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Customer Personal Data by Google in accordance with these Data Processing Terms.

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) Customer Personal Data for the purpose of providing the Processor Services and any related technical support to Customer in accordance with these Data Processing Terms.

Types of Personal Data

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

Categories of Data Subjects

Customer 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 Customer.

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

Google

Privacy Policy

Business Data Responsibility

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

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 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. 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

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.

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. Customer'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,

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 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

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 Customer Personal Data are required to complete additional requirements appropriate to their role. Google's personnel will not process Customer 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).

Google

Privacy Policy

Business Data Responsibility

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 Customer 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.

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

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

Google Privacy Policy

Business Data Responsibility

Data), and (c) the law of Switzerland (if the Swiss FDPA applies to the processing of Customer Personal Data).

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

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

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

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

"**SCCs (Processor-to-Processor, Google Exporter)**" means the terms at business.safety.google/adsprocessorterms/sccs/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 Customers. If Customer is a processor, Customer 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 Customer 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 Customer if, in Google's

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 **Customer's Audit Rights**.

(a) Google will allow Customer or a third party auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under these Data Processing Terms 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 Customer (or a third-party auditor appointed by Customer) 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) Customer 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 Customer 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 Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any third party auditor appointed by Customer to execute any such audit.

(e) Nothing in these Data Processing Terms will require Google either to disclose to Customer or its third party auditor, or to allow Customer or its third party auditor to access: (i) any data of any other 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 Customer or any third party; or (v) any information that Customer or its third party auditor seeks to access for any reason other than the good faith fulfilment of Customer'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 an Alternative Transfer Solution in order to process Customer Personal Data in or transfer it to an Adequate Country. If Customer Personal Data is transferred to any other country, and European Data Protection Legislation applies to the transfers ("**Restricted European Transfers**"), then:

(a) if Google has adopted an Alternative Transfer Solution for any Restricted European Transfers, then Google will inform Customer 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 informs Customer 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 Customer's address is not in an Adequate Country, the SCCs

Processor) and/or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to such Restricted European Transfers between Customer and Google.

7.2 **Supplementary Measures and Information**. Google will provide Customer with information relevant to Restricted European Transfers, including information about supplementary measures to protect Customer 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 Customer Personal Data (for example, help centre articles).

7.3 **Termination**. If Customer 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 Customer Personal Data, then Customer may immediately terminate the Agreement for convenience by notifying Google in writing.

7.4 **Alternative Transfer Solution Adoption and Certification**. Information about Google and/or its Affiliates' adoption of, or certification under, any Alternative Transfer Solutions can be found at https://business.safety.google/adsdatatransfers.

8. Subprocessors. When engaging any Subprocessor, Google will ensure via a written contract that if the processing of Customer 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.

Customer 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 Customer SCCs, Customer's Supervisory Authority; and

Google Privacy Policy

Business Data Responsibility

10. SCCs

10.1 **Order of Precedence**. If there is any conflict or inconsistency between the Customer SCCs and this Appendix 3A, the remainder of these Data Processing Terms or the remainder of the Agreement, then the Customer 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 may offer and Customer may enable certain in-product settings, configurations or other functionality for the Processor Services relating to restricted data processing, as described in supporting documentation available at business.safety.google/rdp, as updated from time to time ("**Restricted Data Processing**"). This Appendix 3B reflects the parties' agreement on the processing of Customer 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

Personal Data as permitted under US State Privacy Laws for service providers and processors.

(c) "**RDP Services**" means Processor Services operating under Restricted Data Processing.

(d) 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.

(e) Customer is solely liable for its compliance with each of the US State Privacy Laws in its use of Google services, including Restricted Data Processing.

3. Applicable State Privacy Law Terms (under Restricted Data Processing).

3.1 With respect to Customer Personal Data processed under Restricted Data Processing, and to the extent that one or more of the US State Privacy Laws applies to the processing of Customer 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 Customer Personal Data, subject to the following modifications:

(1) All references to "Processor Services" are replaced with "RDP Services"; and

(2) The "Types of Personal Data" section is replaced with the following language: "Customer Personal Data may include the types of personal data described under the US State Privacy Laws."

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

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

paragraph 3.4 (Subcontractors) of this Appendix 3B.

(ii) Customer will immediately forward to the relevant controller any notice provided by Google under Section 7.2.1 (Incident Notification) of these Data Protection Terms and paragraph 3.4 (Subcontractors) of this Appendix 3B.

(iii) Customer may make available to the relevant controller any information made available by Google under paragraphs 3.2(b) (Customer's Audit Rights) and 3.4 (Subcontractors) of this Appendix 3B.

3.1.2 **Customer's Instructions for RDP Services.** By entering into this Appendix 3B, and with respect to the RDP Services, Customer instructs Google to process Customer Personal Data only in accordance with the RDP Instructions.

3.1.3 **Google's Compliance with RDP Instructions.** With respect to the RDP Services, Google will comply with the RDP Instructions unless prohibited under the US State Privacy Laws.

3.1.4 **Additional Products.** If Customer uses any product, service or application provided by Google or a third party that: (a) is not part of the RDP Services; and (b) is accessible for use within the user interface of the RDP Services or is otherwise integrated with the RDP Services (an "**Additional Product**"), the RDP Services may allow that Additional Product to access Customer Personal Data as required for the interoperation of the Additional Product with the RDP Services. For clarity, this Appendix 3B does not apply to the processing of personal data in connection with the provision of any Additional Product used by Customer, including personal data transmitted to or from that Additional Product.

3.2 **Data Security**

3.2.1 **Customer's Security Responsibilities and Assessment.**(a)**Customer's Security Responsibilities.** In addition to Customer's security responsibilities under Section 7.3.1 of these Data Processing Terms, Customer agrees that, without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures and Assistance) and 7.2 (Data Incidents) of these Data Processing Terms, Customer is responsible for its use of the RDP Services, including: (1) making appropriate use of

Google

Privacy Policy

Business Data Responsibility

(i) Customer 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 Customer and Google) within 12 months as of the date of Customer's request and (2) any other information Google determines is reasonably necessary for Customer to verify such compliance.

(ii) Alternatively, Google may, at its sole discretion and in response to a request by Customer, 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. Where Customer requests such an audit, Google may charge a fee (based on Google's reasonable costs) for any audit. Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any third-party auditor appointed by Customer to execute any such audit.

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

(1) any data of any other customer 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 Customer or any third party; or

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

3.4 **Subcontractors.**

(a) Customer generally authorizes Google to engage other entities as subcontractors in connection with the provision of the RDP Services. When engaging any subcontractor, Google will:

(i) ensure via a written contract that: (A) the subcontractor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this Appendix 3B); and (B) if the processing of Customer Personal Data is subject to the US State Privacy Laws, ensure that the data protection obligations in this Appendix 3B are imposed on the subcontractor;

(ii) when engaging any new subcontractors, provide notice of such new subcontractors where required by US State Privacy Laws, and, where required by US State Privacy Laws, further provide an opportunity for Customer to object to such subcontractors; and

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

(b) Customer may object to any new subcontractor by terminating the Agreement for convenience immediately upon written notice to Google, on condition that Customer provides such notice within 90 days of being informed of the engagement of the new subcontractor as described in paragraph 3.4(a)(ii) herein.

4. US State Privacy Law Terms

4.1 **Deidentified Data.** With respect to Customer Personal Data processed with or without Restricted Data Processing enabled, and to the extent that one or more of the US State Privacy Laws applies to the processing of Customer 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), Customer Personal Data means any personal data that is

Google

Privacy Policy

Business Data Responsibility

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

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

(ii) Google will not retain, use or disclose Customer Personal Data (including outside of the direct business relationship between Google and Customer), other than for a business purpose under the CCPA on behalf of Customer and the specific purpose of performing the RDP Services, as further described in supporting documentation available at business.safety.google/rdp, as updated from time to time;

(iii) Google will not combine Customer Personal Data that Google receives from, or on behalf of, Customer with (a) personal information that Google receives from, or on behalf of, another person or persons or (b) personal information collected from Google's own interaction with a consumer, as further described in supporting documentation available at business.safety.google/rdp except to the extent permitted under CCPA;

(iv) Google will process such Customer Personal Data for the specific purpose of performing the RDP 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 Customer is making such Customer Personal Data available to Google for such purposes;

(v) Google will allow audits to verify Google's compliance with its obligations under this Appendix 3B in accordance with paragraph 3.2.1(b) (Customer's Audit Rights) of this Appendix 3B;

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

Google

Privacy Policy

Business Data Responsibility

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

5.2 With respect to Customer Personal Data processed without Restricted Data Processing enabled, and to the extent that CCPA applies to the processing of Customer Personal Data:

(i) Google will process such Customer 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 Customer is making such Customer Personal Data available to Google for such purposes;

(ii) Google will allow audits to verify Google's compliance with its obligations under this Appendix 3B in accordance with paragraph 3.2.1(b) (Customer's Audit Rights) herein.

(iii) Google will notify Customer if Google makes a determination that it can no longer meet its obligations under the CCPA;

(iv) If Customer reasonably believes that Google is processing Customer Personal Data in an unauthorized manner, Customer has the right to notify Google of such belief via the methods described at privacy.google.com/businesses/processorsupport, and the parties will work together in good faith to remediate the allegedly violative processing activities, if necessary; and

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

6. **Changes to this Appendix 3B.** In addition to Section 15 of the Data Processing Terms (Changes to these Data Processing Terms), 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 Customer under the US State Privacy Laws, as reasonably determined by Google.

Google

Privacy Policy

Business Data Responsibility

- 1 September 2023
- 1 July 2023
- 1 January 2023
- 21 September 2022
- 27 September 2021
- 16 August 2020
- 12 August 2020
- 1 January 2020
- 31 October 2019
- 12 October 2017