DATA PROCESSING AND SECURITY ADDENDUM FOR LOOKER TECHNICAL PERSONNEL SERVICES

This Addendum will not apply if Customer's most recent data processing document for the Looker Application is an offline Data Protection Addendum signed by Google (including as successor-in-interest of Looker Data Sciences, Inc.) and Customer. If you are accessing the Technical Personnel Services from Google as a customer of an unaffiliated Google Cloud Platform reseller, if the Looker Terms of Service are referenced in your agreement with your reseller, this Addendum will govern your use of the Technical Personnel Services and is applicable as between you and the reseller.

Last modified: January 4, 2022

1. Introduction

This Data Processing and Security Addendum for Looker Technical Personnel Services (the "*Addendum*") reflects the parties' agreement with respect to the processing and security of Customer Personal Data in relation to Google's provision of Technical Personnel Services to the Customer. This Addendum (i) supplements the Personnel Agreement (as defined below); (ii) supplements the Looker Application Agreement (as defined below) to the extent set forth in the immediately following paragraph; and (iii) does not apply to the processing or security of Customer Data by the Looker Application.

If Customer's Looker Application Agreement does not have data protection terms governing the Looker Application, and the processing of Customer Personal Data under the Personnel Agreement is subject to data protection laws, the Looker Data Processing and Security Terms at https://looker.com/trust-center/legal/customers/dpst/ will apply to Customer's use of the Looker Application during the Term of the Personnel Agreement (inclusive of this Addendum).

Customer represents and warrants (1) that in order to receive the Technical Personnel Services, Customer has a lawful basis to process, and to instruct Google to process, Customer Personal Data and (2) Customer will not use any part of the Technical Personnel Services for 'automated individual decision-making' (as defined in GDPR) with respect to Customer Personal Data.

2. Definitions

2.1 Capitalized terms defined in the Personnel Agreement apply to this Addendum. In addition, in this Addendum:

- *Addendum Effective Date* means the date Customer accepted, or the parties otherwise agreed to, this Addendum.

- *Adequate Country means:*

  (a) for data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR;

  (b) for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or

  (c) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is 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) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.

- *Customer means the non-Google entity agreeing to the Personnel Agreement and the Looker Application Agreement.*

- *Customer Data* means all (a) data in Customer's databases provided to Google by Customer or End Users via the Services and (b) results provided to Customer or End Users for queries executed against such data via the Services, in each case that is (i) provided by or on behalf of Customer to Google via a Customer Instance of the Looker Application, and (ii) processed by Google personnel performing Technical Personnel Services under the Personnel Agreement.

- *Customer Personal Data* means the personal data contained within the Customer Data, including any special categories of personal data defined under European Data Protection Law.

- *Data Incident* means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

- *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 Law* means, as applicable: (a) the GDPR; and/or (b) the Swiss FDPA.

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

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

- *Instance or Customer's Instance* means an authorized deployment of downloadable tools or an online software application, including the licensed Looker data platform and other computer software provided by Google, installed on a single operating system.

- *Instructions* has the meaning given in Section 5.2.1 (Customer's Instructions).

- *Looker Application* means an integrated platform that includes optional cloud-based infrastructure as well as software components (which may include associated APIs) and enables businesses to analyze data and define business metrics across multiple data sources.

- *Looker Application Agreement* means the agreement between Customer and Google that governs Customer's use of the Looker Application.

- *Looker CE Services* means the advisory and consulting services provided by Google to Customer for a trial or pre-sales engagement of the Looker Application.

- *New Subprocessor* has the meaning set forth in Section 11.1 (Consent to Subprocessor Engagement).

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

- *Notification Email Address* means the email address(es) designated by Customer in the Order Form to receive certain notifications from Google; except that for Looker CE Services, it means the email address provided by Customer to Google in another written form (email or other electronic means permitted) as authorized by Google. Customer is responsible for giving Google timely notice of any changes to the email address(es) so designated and for ensuring that its Notification Email Address remains current and valid.

- *Order Form* means an order form or other document issued by Google and executed by Customer and Google specifying the Technical Personnel Services Google will provide to Customer.

- *Personnel Agreement* means one of the following agreements to the extent it governs the Technical Support Services:

  (i) Looker Application Agreement; or

  (ii) Implementation Services Agreement; or

  (iii) an Order Form or Statement of Work referencing another agreement between Google and Customer, and incorporating this Addendum by reference.

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

- *Subprocessor* means a third party authorized as another processor under Section 11 (Subprocessors) of this Addendum to have logical access to and process Customer Personal Data in order to provide parts of the Looker Application.

- *Subprocessor URL* has the meaning given in Section 11.2 (Information about Subprocessors).

- *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).

- *Technical Personnel Services* means, when provided in Customer's Instance of the Looker Application: (i) the advisory and consulting services described in an Order Form, which may include a Statement of Work, (ii) applicable technical support services as described at /trust-center/legal/customers/support-lss, or (iii) Looker CE Services.

- *Term* means the period from the effective date of the Personnel Agreement until the time Customer removes, or allows to expire, Google's access to the Customer Instance for Technical Personnel Services.

- *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 "*personal data*", "*data subject*", "*processing*", "*controller*" and "*processor*" as used in this Addendum have the meanings given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

3. Duration

This Addendum will, notwithstanding any earlier expiry of the Term, remain in effect until, and automatically expire upon, termination of Google personnel's access to Customer Personal Data in Customer's Instance of the Looker Application. Customer is responsible for terminating access to Customer Personal Data provided to Google personnel via Customer's Instance of the Looker Application upon completion of the Technical Personnel Services.

4. Scope of Data Protection Law

4.1 *Application of European Law*. The parties acknowledge that European Data Protection Law will apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or

b. the Customer 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 in the EEA or the UK, or the monitoring of their behavior in the EEA or the UK.

4.2 *Application of Non-European Data Protection Law*. The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.

4.3 *Application of Terms*. Except to the extent this Addendum states otherwise, this Addendum will apply as long as Customer uses Technical Personnel Services, irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

5. Processing of Data

5.1 *Roles and Regulatory Compliance; Authorization*.

5.1.1 *Processor and Controller Responsibilities*. If European Data Protection Law applies to the processing of Customer Personal Data:

a. the subject matter and details of the processing are described in Appendix 1;

b. Google is a processor of that Customer Personal Data under European Data Protection Law;

c. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and

d. each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.

5.1.2 *Processor Customers*. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants on an ongoing basis that the relevant controller has authorized: (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). Customer will immediately forward to the relevant controller any notice provided by Google under Sections 5.2.3 (Instruction Notifications), 7.2.1 (Incident Notification), 9.2 (Data Subject Requests), 11.4 (Opportunity to Object to Subprocessor Changes), or that refers to any requests related to standard contractual clauses.

5.1.3 *Responsibilities under Non-European Law*. If Non-European Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

5.2 *Scope of Processing*.

5.2.1 *Customer's Instructions*. Customer instructs Google to process Customer Personal Data only: in accordance with applicable law: (a) to provide, secure and monitor the Technical Personnel Services; (b) as documented in the Personnel Agreement and this Addendum; and (c) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Addendum (collectively, the "*Instructions*").

5.2.2 *Google's Compliance with Instructions*. Google will comply with the Instructions unless prohibited by European Law.

5.2.3 *Instruction Notifications*. Google will immediately notify Customer if, in Google's opinion: (a) European Law prohibits Google from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Law; or (c) Google is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law. This Section does not reduce either party's rights and obligations elsewhere in the Personnel Agreement.

6. Data Deletion

Taking into account the nature of the processing of Customer Personal Data under the Personnel Agreement, the parties' respective rights and obligations with respect to deletion of

Customer Personal Data after expiry of the Term are addressed in the Looker Application Agreement.

7. Data Security

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

7.1.1 *Google's Security Measures*. Taking into account the nature of the processing of Customer Personal Data under the Personnel Agreement, Google will implement and maintain technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "*Security Measures*").

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

7.1.3 *Google's Security Assistance*. Taking into account the nature of the processing of Customer Personal Data under this Addendum, Customer's security obligations and Google's assistance with such obligations under the GDPR with respect to Customer Personal Data on the Looker Application are addressed separately in the Customer's Looker Application Agreement.

7.2 *Data Incidents*.

7.2.1 *Incident Notification*. Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and will promptly take reasonable steps to minimize harm and secure Customer Personal Data.

7.2.2 *Details of Data Incident*. Google's notification of a Data Incident 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*. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address, or, at Google's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4 *No Assessment of Customer Data by Google*. Google has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

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*. Without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), Customer agrees that Customer is responsible for its use of the Technical Personnel Services, including without limitation:

a. using the security controls in the Looker Application to ensure a level of security appropriate to the risk to Customer Personal Data;
b. providing Google with the minimum amount of Customer Personal Data necessary for Google to provide the Technical Personnel Services;
c. securing the account authentication credentials, systems and devices Customer uses to receive the Technical Personnel Services;
d. backing up its Customer Data as appropriate;
e. providing instructions on Google's use and processing of Customer Personal Data; and
f. to the extent Google's access to Customer Personal Data is within Customer's control, terminating Google's access to Customer Personal Data on the earlier of completion of the Technical Personnel Services or the completion of the purpose for which Customer Personal Data is provided to Google under the Personnel Agreement.

Google has no obligation to protect copies of Customer Data that Customer stores outside of Customer's Instance (for example, offline or on-premises storage).

7.3.2 *Customer's Security Assessment*. Customer agrees that the Technical Personnel Services, the Security Measures implemented and maintained by Google, and Google's commitments under this Section 7 (Data Security) and Section 11 (Subprocessors) provide a level of security appropriate to the risk to Customer 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 Compliance Certification and SOC Report. Taking into account the nature of the processing of Customer Personal Data under this Addendum, Google's security certifications (which apply to the Looker Application) are addressed separately in the Looker Application Agreement.

7.5 *Reviews and Audits of Compliance*. Taking into account the nature of the processing of Customer Personal Data under this Addendum, Customer's audit rights with respect to Customer Personal Data are addressed separately in the Looker Application Agreement.

8. Impact Assessments and Consultations

Customer agrees that Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations under Articles 35 and 36 of the GDPR upon Customer's request by providing Customer with reasonable cooperation and assistance.

9. Access; Data Subject Rights; Data Export

9.1 *Access; Rectification; Restricted Processing; Portability*. Taking into account the nature of the processing of Customer Personal Data under this Addendum, Customer's ability to access, rectify and restrict processing of Customer Personal Data is addressed separately in the Looker Application Agreement.

9.2 *Data Subject Requests*. Taking into account the nature of the processing of Customer Personal Data under this Addendum, Customer's obligations and Google's assistance with respect to data subject requests related to Customer Personal Data are addressed separately in the Looker Application Agreement.

10. Data Transfers

Taking into account the nature of the processing of Customer Personal Data under this Addendum, if the processing of that Customer Personal Data is subject to European Data Protection Law, the Customer Personal Data may only be transferred to a country that is not an Adequate Country as addressed separately in Customer's Looker Application Agreement.

11. Subprocessors

11.1 *Consent to Subprocessor Engagement*. Customer specifically authorizes the engagement as Subprocessors of: (a) any third party entity listed in an applicable Order Form, Statement of Work or other confirmation provided to a Customer before commencement of the Technical Personnel Services; and (b) all other Google Affiliates from time to time. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement as Subprocessors of any other third parties ("*New Subprocessor*").

11.2 *Information about Subprocessors*. Information about Subprocessors, including their functions and locations will be made available to Customer at Customer's request.

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

a. assess the Subprocessor's security and privacy practices to verify that the Subprocessor provides a level of security and privacy appropriate to the data it will access and the services it will provide;
b. ensure via a written contract that:

    i. 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 Personnel Agreement (including this Addendum); and

    ii. If the processing of Customer Personal Data is subject to European Data Protection Law, the data protection obligations described in this Addendum (as referred to in Article 28(3) of the GDPR if applicable) are imposed on the Subprocessor; and

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

11.4 *Opportunity to Object to Subprocessor Changes*.

a. When any New Subprocessor is engaged during the Term, Google will notify Customer of the engagement of the New Subprocessor before the New Subprocessor processes Customer Personal Data.
b. Customer may object to the New Subprocessor and request a change of Personnel in accordance with the Personnel Agreement. The parties will work in good faith to determine a satisfactory alternative.

12. Cloud Data Protection Team; Processing Records

Google will keep appropriate documentation of its processing activities as required by the GDPR. To the extent the GDPR requires Google to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Google and keep it accurate and up-to-date. Google may make any such information available to the Supervisory Authority if required by the GDPR.

13. Interpretation; Precedence

To the extent of any conflict or inconsistency between this Addendum and the remainder of the Personnel Agreement or Looker Application Agreement (if applicable), this Addendum will prevail.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Technical Personnel Services to Customer.

Duration of the Processing

The Term plus any period from the expiry of the Term to Customer's termination of access to Customer Data by Google for Technical Personnel Services.

Nature and Purpose of the Processing for the Technical Personnel Services

Google will process Customer Personal Data for the purposes of providing the Technical Personnel Services to Customer.

Categories of Data

Data relating to individuals provided to Google for Technical Personnel Services under the Personnel Agreement or Looker Application Agreement (as applicable) by (or at the direction of) Customer.

Data Subjects

Data subjects include the individuals about whom data is provided to Google by (or at the direction of) Customer via the Customer Instance for Technical Personnel Services.

Appendix 2: Security Measures

As from the Addendum Effective Date, Google will implement and maintain the Security Measures set out in this Appendix 2.

1. Access to Customer Personal Data

Google will only access and process Customer Personal Data provided to Google by Customer in a Customer controlled Looker Application. Customer's use of the Looker Application is governed by the Looker Application Agreement, including any applicable security measures.

2. Internal Data Access Processes and Policies

Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to track any access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos, DUO and a proprietary system utilizing SSH 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 minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information , Google uses hardware tokens.

3. 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 (eg., certifications). Google's personnel will not process Customer Personal Data without authorization.

4. Additional Security Measures. Looker and Customer may agree to additional security measures in the applicable Order Form, including any attached Statement of Work, for the Technical Personnel Services.