11. Notwithstanding anything to the contrary in this Data Processing Addendum, Pa8ner may provide, at its own expense, personal data of others to Google (collectively with Pa8ner Personal Data, "Data") in connection with the Processor Services, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

12. Categories of Data Subjects

6. Nature and Purpose of the Processing

7. Data Processing Addendum for Products where Google is a Data Processor

15. Effect of this Data Processing Addendum

11.1 Notification of Changes.

11.2 If the Agreement is governed by the laws of:

(a) the GDPR; or

(b) the Swiss FDPA; and

15.3 Alternative Transfer Solution

7.3.1 Data Incidents.

11.3 Google’s Compliance with Instructions.

7.2.2 Assistance.

7.1.1 Data, as described in Section 5.3 (Google’s Compliance with Instructions); and (iii) otherwise have a material adverse impact on Pa8ner’s rights under this Agreement. Pa8ner 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).

11.4 Data Incidents.

11.5 Pa8ner agrees that, as of their effective date, the SCCs will supersede and terminate any Model Contract Clauses approved under Article 26(2) of European Data Protection Legislation, in each case in a manner that does not affect the validity of the Standard Contractual Clauses adopted under the European Data Protection Legislation, in each case in a manner that does not affect the validity of the Standard Contractual Clauses.
The following Additional Terms for Non-European Data Protection Legislation supplement these Data Processing Terms:

2. Updates and Modifications

Time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

4 May 2018

31 October 2019

2. Personnel Security

Before onboarding Subprocessors, Google conducts an audit of the Subprocessors’ security and privacy practices to ensure Subprocessors provide a level of security and statutory regulations. Personnel are provided with security training. Personnel handling Personal Data are required to complete additional requirements appropriate to their role. Google’s policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.”

3. Data Access Controls

Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in buildings which are designed to meet the physical security requirements for a data center. The data centers are required to be secured by perimeter intrusion detection and alarm systems which are connected to Google’s central security operations center. These systems are designed to detect any unauthorized access attempts to the data centers. Google personnel are required to have a personnel security background check as part of the training package for its personnel and to complete additional requirements appropriate to their role. 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 any security incidents.

Access Control and Identity Management – Access Policy. Google’s internal data access processes and policies are designed to prevent unauthorised persons from accessing Personal Data. Google implements a centralised access management system to control personnel access to Google’s data centers 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 personal data; (ii) log all access to personal data and/or systems; (iii) identify, contact, or precisely locate an individual); such as a user’s Google account data. Google policies only allow for information flows between pseudonymous data and personally identifiable user information (i.e. information that could be used on its own to directly identify an individual).

Pseudonymous Data. Online advertising data are commonly associated with online identifiers which on their own are considered ‘pseudonymous’ (i.e. they cannot uniquely identify an individual). Google allows for information flows between pseudonymous data and personally identifiable user information (i.e. information that could be used on its own to directly identify an individual). These policies ensure the separation between pseudonymous data and personally identifiable user information (i.e. information that could be used on its own to directly identify an individual).

3. Data

Google’s security policies mandate encryption at rest for all user data, including personal data. Data is encrypted at multiple levels in transit and at rest. Google’s security policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.

3. Data

Google’s security policies mandate encryption at rest for all user data, including personal data. Data is encrypted at multiple levels in transit and at rest. Google’s security policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.

2. Data

Google’s security policies mandate encryption at rest for all user data, including personal data. Data is encrypted at multiple levels in transit and at rest. Google’s security policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.

3. Data

Google’s security policies mandate encryption at rest for all user data, including personal data. Data is encrypted at multiple levels in transit and at rest. Google’s security policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.

2. Data

Google’s security policies mandate encryption at rest for all user data, including personal data. Data is encrypted at multiple levels in transit and at rest. Google’s security policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.

3. Data

Google’s security policies mandate encryption at rest for all user data, including personal data. Data is encrypted at multiple levels in transit and at rest. Google’s security policies also cover the physical security of Google’s facilities and the data centers. To ensure the protection of Personal Data, access to Google’s data centers is limited to Google internal personnel, contractors, and subcontractors.