

- [Back to Google Cloud Terms Directory](#)
- >
- Current

## Cloud Data Processing Addendum (Customers)

This Cloud Data Processing Addendum including its appendices (the “*Addendum*”) is incorporated into the Agreement(s) under which Google has agreed to provide Google Cloud Platform, Google Workspace, or Cloud Identity (each as defined below), as applicable (the “*Services*”), to Customer. This Addendum was formerly known as the “Data Processing and Security Terms” under an Agreement for Google Cloud Platform and the “Data Processing Amendment” under an Agreement for Google Workspace or Cloud Identity.

### 1. Commencement

This Addendum will be effective and replace any terms previously applicable to the processing of Customer Data, including any Data Processing and Security Terms or Data Processing Amendment, from the Addendum Effective Date (as defined below).

### 2. Definitions

2.1 Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement:

- *Account* has the meaning given in the applicable Agreement or, if no such meaning is given, means Customer’s Google Cloud Platform account, Google Workspace account or Cloud Identity account, as applicable.
- *Addendum Effective Date* means the date on which Customer accepted, or the parties otherwise agreed to, this Addendum.
- *Additional Security Controls* means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including the Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- *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 Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.

- *Audited Services* means the then-current Services indicated as being in-scope for the relevant certification or report at <https://cloud.google.com/security/compliance/services-in-scope>. Google may not remove any Services from this URL unless those Services have been discontinued in accordance with the applicable Agreement.
- *Cloud Identity* means the Cloud Identity Services described at <https://cloud.google.com/terms/identity/user-features>, when purchased under a standalone Agreement.
- *Customer Data* has the meaning given in the applicable Agreement or, if no such meaning is given, means:
  - (a) data provided by or on behalf of Customer or its End Users via Google Cloud Platform under the Account; or
  - (b) data submitted, stored, sent or received by or on behalf of Customer or its End Users via Google Workspace or Cloud Identity under the Account.
- *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.
- *Customer SCCs* means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor) and/or the SCCs (Processor-to-Controller), as applicable.
- *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 Data on systems managed by or otherwise controlled by Google.
- *EEA* means the European Economic Area.
- *EMEA* means Europe, the Middle East and Africa.
- *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.
- *Google Cloud Platform* means the Google Cloud Platform services described at <https://cloud.google.com/terms/services>, excluding any Third-Party Offerings.
- *Google Workspace* means the Google Workspace or Google Workspace for Education services described at [https://workspace.google.com/terms/user\\_features.html](https://workspace.google.com/terms/user_features.html), as applicable.
- *Google's Third Party Auditor* means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.
- *Instructions* has the meaning given in Section 5.2.1 (Compliance with Customer's Instructions).
- *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 Admin Console or Order Form to receive certain notifications from Google. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.

- *SCCs* means the Customer SCCs and/or SCCs (Processor-to-Processor, Google Exporter), as applicable.
- *SCCs (Controller-to-Processor)* means the terms at: <https://cloud.google.com/terms/scs/eu-c2p>
- *SCCs (Processor-to-Controller)* means the terms at: <https://cloud.google.com/terms/scs/eu-p2c>
- *SCCs (Processor-to-Processor)* means the terms at: <https://cloud.google.com/terms/scs/eu-p2p>
- *SCCs (Processor-to-Processor, Google Exporter)* means the terms at: <https://cloud.google.com/terms/scs/eu-p2p-google-exporter>
- *Security Documentation* means all documents and information made available by Google under Section 7.5.1 (Reviews of Security Documentation).
- *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 this Addendum to have logical access to and process Customer Data in order to provide parts of the Services and TSS.
- *Supervisory Authority* means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR and/or the Swiss FDPA.
- *Swiss FDPA* means the Federal Data Protection Act of 19 June 1992 (Switzerland).
- *Term* means the period from the Addendum Effective Date until the end of Google's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.
- *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

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google deletes all Customer Data as described in this Addendum.

### 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:

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

4.3 *Application of Addendum.* Except to the extent this Addendum states otherwise, this Addendum will apply 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:

- a. 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);
- b. Customer will immediately forward to the relevant controller any notice provided by Google under Sections 5.2.2 (Instruction Notifications), 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), 11.4 (Opportunity to Object to Subprocessor Changes) or that refers to any SCCs; and
- c. Customer may:
  - i. request access for the relevant controller to the SOC Reports in accordance with Section 7.5.3(a); and
  - ii. make available to the relevant controller any other information made available by Google under Sections 10.4 (Supplementary Measures and Information), 10.6 (Data Center Information) and 11.2 (Information about Subprocessors).

**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 Compliance with Customer's Instructions.** Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) and applicable law only: (a) to provide, secure, and monitor the Services and TSS; and (b) as further specified via (i) Customer's use of the Services (including the Admin Console and other Services functionality) and TSS, and (ii) any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum (collectively, the "Instructions"). Google will comply with the Instructions unless prohibited by European Law.

**5.2.2 Instruction Notifications.** Without prejudice to Google's obligations under Section 5.2.1 (Compliance with Customer's Instructions) or any other rights or obligations of either party under the applicable Agreement, 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.



**5.3 Additional Products.** If Google at its option makes Additional Products available to Customer for use with Google Workspace or Cloud Identity in accordance with applicable Additional Product Terms:

- a. Customer may enable or disable Additional Products via the Admin Console and will not need to use Additional Products in order to use Google Workspace or Cloud Identity; and
- b. if Customer opts to install any Additional Products or to use them with Google Workspace or Cloud Identity, the Additional Products may access Customer Data as required to interoperate with Google Workspace or Cloud Identity (as applicable).

For clarity, this Addendum does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products.

## 6. Data Deletion

**6.1 Deletion by Customer.** Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.

**6.2 Return or Deletion When Term Ends.** If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google's systems at the end of the Term in accordance with applicable law. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.

**6.3. Deferred Deletion Instruction.** To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Return or Deletion When Term Ends) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will take effect with respect to such Customer Data only when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its deletion by Google.

## 7. Data Security

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

**7.1.1 Google's Security Measures.** Google will implement and maintain technical, organizational and physical measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). The Security Measures include measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

**7.1.2 Access and Compliance.** Google will: (a) authorize its employees, contractors and Subprocessors to access Customer 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 Subprocessors to the extent applicable to their scope of performance; and (c) ensure that all persons authorized to process Customer Data are under an obligation of confidentiality.

**7.1.3 Additional Security Controls.** Google will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing,

accessing and using Customer Data.

**7.1.4 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 its (or, where Customer is a processor, the relevant controller's) obligations under Articles 32 to 34 of the GDPR, by:

- a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);
- b. making Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);
- c. complying with the terms of Section 7.2 (Data Incidents);
- d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement (including this Addendum); and
- e. if subsections (a)-(d) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

## **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 promptly take reasonable steps to minimize harm and secure Customer 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.

**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), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Google's or Google's Subprocessors' systems, including:

- a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to the Customer Data;
- b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and
- c. backing up or retaining copies of its Customer Data as appropriate.

*7.3.2 Customer's Security Assessment.* Customer agrees that the Services, Security Measures implemented and maintained by Google, Additional Security Controls and Google's commitments under this Section 7 (Data Security) 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 Certifications and SOC Reports.* Google will maintain at least the following for the Audited Services in order to evaluate the continued effectiveness of the Security Measures: (a) certificates for ISO 27001, ISO 27017 and ISO 27018 and, for Google Cloud Platform, a PCI DSS Attestation of Compliance (the "Compliance Certifications"); and (b) SOC 2 and SOC 3 reports produced by Google's Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the "SOC Reports"). Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

### *7.5 Reviews and Audits of Compliance.*

*7.5.1 Reviews of Security Documentation.* Google will make the Compliance Certifications and the SOC Reports available for review by Customer to demonstrate compliance by Google with its obligations under this Addendum.

#### *7.5.2 Customer's Audit Rights.*

- a. If European Data Protection Law applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Addendum in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Google will make available all information necessary to demonstrate such compliance and contribute to the audit as described in Section 7.4 (Compliance Certifications and SOC Reports) and this Section 7.5 (Reviews and Audits of Compliance).
- b. If Customer SCCs apply as described in Section 10.2 (Restricted European Transfers), Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).
- c. Customer may conduct an audit to verify Google's compliance with its obligations under this Addendum by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third Party Auditor).

#### *7.5.3 Additional Business Terms for Reviews and Audits.*

- a. Customer must send any requests for reviews of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1, or audits under Section 7.5.2(a) or 7.5.2(b), to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).
- b. Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) or 7.5.2(b).
- c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) or 7.5.2(b). Google will provide 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 auditor appointed by Customer to execute any such audit.
- d. Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) or 7.5.2(b) if the auditor is, in Google's reasonable opinion, not suitably qualified

or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.

## 8. Impact Assessments and Consultations

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, by:

- a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation);
- b. providing the information contained in the applicable Agreement (including this Addendum); and
- c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

## 9. Access etc.; Data Subject Rights; Data Export

**9.1 Access; Rectification; Restricted Processing; Portability.** During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by applicable European Data Protection Law.

### 9.2 Data Subject Requests.

**9.2.1 Responsibility for Requests.** During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

**9.2.2 Google's Data Subject Request Assistance.** Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

- a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);
- b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and
- c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

## 10. Data Transfers

**10.1 Data Storage and Processing Facilities.** Subject to Google's data location commitments under the Service Specific Terms and the remainder of this Section 10 (Data Transfers), Customer Data may be processed in any country in which Google or its Subprocessors maintain facilities.

**10.2 *Restricted European Transfers.*** The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection Law applies to the transfers (as certified by Customer under Section 10.3 (Certification by Non-EMEA Customers) if its billing address is outside EMEA) (â€œ*Restricted European Transfers*â€), 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 it; 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 Googleâ€™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 Customerâ€™s billing address is not in an Adequate Country, the SCCs (Processor-to-Controller) will apply (regardless of whether Customer is a controller and/or processor) with respect to such Restricted European Transfers between Google and Customer; or

ii. if Googleâ€™s address is not in an Adequate Country, the SCCs (Controller-to-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 Google and Customer.

**10.3 *Certification by Non-EMEA Customers.*** If Customerâ€™s billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, Customer will certify as such, and identify its competent Supervisory Authority, via the Admin Console for Google Cloud Platform or Google Workspace and Cloud Identity, as applicable.

**10.4 *Supplementary Measures and Information.*** Google will provide Customer with information relevant to Restricted European Transfers, including information about Additional Security Controls and other supplementary measures to protect Customer Personal Data:

a. as described in Section 7.5.1 (Reviews of Security Documentation);

b. in the documentation for the Services, available at <https://cloud.google.com/docs>; and

c. in the Google Cloud Trust and Security website, available at <https://cloud.google.com/security>.

**10.5 *Termination.*** If Customer concludes, based on its current or intended use of the 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 applicable Agreement for convenience by notifying Google.

**10.6 *Data Center Information.*** The locations of Google data centers are described at:

a. <https://cloud.google.com/about/locations/> for Google Cloud Platform; and

b. <https://www.google.com/about/datacenters/locations/> for Google Workspace and Cloud Identity.

## **11. Subprocessors**

**11.1 *Consent to Subprocessor Engagement.*** Customer specifically authorizes the engagement as Subprocessors of those entities disclosed under Section 11.2 (Information about Subprocessors) as of the



Addendum Effective Date. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement of other third parties as Subprocessors (â€œNew Subprocessorsâ€).

11.2 *Information about Subprocessors.* Names, locations and activities of Subprocessors are described at:

- a. <https://cloud.google.com/terms/subprocessors> for Google Cloud Platform; and
- b. <https://workspace.google.com/intl/en/terms/subprocessors.html> for Google Workspace and Cloud Identity.

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

- a. ensure via a written contract that:
  - i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable 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
- b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 *Opportunity to Object to Subprocessor Changes.*

- a. When any New Subprocessor is engaged during the Term, Google will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location and activities of the New Subprocessor).
- b. Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by immediately terminating the applicable Agreement for convenience by notifying Google.

## 12. Cloud Data Protection Team; Processing Records

12.1 *Cloud Data Protection Team.* Googleâ€™s Cloud Data Protection Team will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Data under the applicable Agreement and can be contacted:

- a. at <https://support.google.com/cloud/contact/dpo> for Google Cloud Platform;
- b. at [https://support.google.com/a/contact/googlecloud\\_dpr](https://support.google.com/a/contact/googlecloud_dpr) for Google Workspace and Cloud Identity (while Administrators are signed in to their Admin Account); or
- c. as described in the Notices section of the applicable Agreement.

12.2 *Googleâ€™s 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 use the Admin Console to supply such information and keep it accurate and up-to-date. Google may make any such information available to the Supervisory Authorities if required by the GDPR.

12.3 *Controller Requests.* During the Term, if Googleâ€™s Cloud Data Protection Team receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Google will advise the third party to contact Customer.

## 13. Interpretation

### 13.1 *Precedence.*

- a. To the extent of any conflict or inconsistency between:
  - i. this Addendum and the remainder of the Agreement, this Addendum will prevail; and
  - ii. any Customer SCCs (which are incorporated by reference into this Addendum) and the remainder of the Agreement (including this Addendum), the Customer SCCs will prevail.
- b. For clarity, if Customer has entered more than one Agreement, this Addendum will amend each of the Agreements separately.

**13.2 *Legacy UK SCCs.*** The supplementary terms for UK GDPR transfers in the SCCs will, as of 21 September 2022, supersede and terminate any standard contractual clauses approved under the UK GDPR or Data Protection Act 2018 and previously entered into by Customer and Google.

**13.3 *No Modification of SCCs.*** Nothing in the Agreement (including this Addendum) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

## **Appendix 1: Subject Matter and Details of the Data Processing**

### *Subject Matter*

Google's provision of the Services and TSS to Customer.

### *Duration of the Processing*

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

### *Nature and Purpose of the Processing*

Google will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with this Addendum.

### *Categories of Data*

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or by its End Users.

### *Data Subjects*

Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or by its End Users.

## **Appendix 2: Security Measures**

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

### **1. Data Center and Network Security**

#### *(a) Data Centers.*

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

*Redundancy.* Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The 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 center equipment is scheduled through a standard change process according to documented procedures.

*Power.* The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 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 center. Backup power is provided by various mechanisms such as uninterruptible power supplies (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 center, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

*Server Operating Systems.* Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

*Businesses Continuity.* Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

#### *(b) Networks and Transmission.*

*Data Transmission.* Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

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

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

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

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

*Encryption Technologies.* Google makes HTTPS encryption (also referred to as SSL or 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 minimize the impact of a compromised key, or a cryptographic breakthrough.

## **2. Access and Site Controls**

### *(a) Site Controls.*

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

*Data Center Access Procedures.* Google maintains formal access procedures for allowing physical access to the data centers. The data centers 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 center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

*On-site Data Center Security Devices.* Google's data centers employ a dual authentication access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers 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 up to 30 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 Services, and responding to security incidents.

*Access Control and Privilege Management.* Customer's administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

*Internal Data Access Processes and Policies – Access Policy.* 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 Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate 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. Google's authentication and authorization systems utilize SSH certificates and security keys, and 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 (e.g. credit card data), Google uses hardware tokens.

### 3. Data

(a) *Data Storage, Isolation and Logging.* Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data and, for Google Workspace and Cloud Identity: (i) Google logically separates each End User's data from the data of other End Users; and (ii) data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

(b) *Decommissioned Disks and Disk Erase Policy.* 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 "Disk Erase Policy") 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 Disk Erase Policy.

### 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 Data are required to complete additional requirements appropriate to their role (e.g. certifications). Google's personnel will not process Customer Data without authorization.

### 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, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement) of this Addendum, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

*Previous versions of Data Processing and Security Terms:*

[June 30, 2022](#) [September 24, 2021](#) [August 19, 2020](#) [August 10, 2020](#) [July 17, 2020](#) [October 11, 2019](#) [October 1, 2019](#) [May 25, 2018](#) [March 13, 2018](#) [November 9, 2017](#) [October 11, 2017](#) [February 7, 2017](#) [October 6, 2016](#)

*Previous versions of Data Processing Amendment:*

[July 7, 2022](#) [September 24, 2021](#) [May 27, 2021](#) [October 29, 2019](#) [May 25, 2018](#) [April 25, 2018](#) [July 11, 2017](#) [November 28, 2016](#) [January 7, 2016](#) [April 24, 2015](#) [April 1, 2014](#) [November 14, 2012](#)

(Last modified September 20, 2022)



