Fabric Data Processing and Security Terms

Terms last modified: June 20, 2019

The customer agreeing to these terms ("Customer"), and Google LLC (formerly known as Google Inc.), Google Ireland Limited, Google Asia Pacific Pte. Ltd., or any other entity that directly or indirectly controls, is controlled by, or is under common control with Google LLC (as applicable, "Google"), have entered into an agreement under which Google has agreed to provide the "Fabric Answers", "Fabric Crashlytics", "Firebase Crashlytics", or "Fabric Beta" products or services to Customer (as amended from time to time, the "Agreement").

These Fabric Data Processing and Security Terms, including their appendices, (the "Terms") will be effective and replace any previously applicable data processing and security terms as from the Terms Effective Date (as defined below). These Terms supplement the Agreement.

1. Introduction

These Terms reflect the parties' agreement with respect to the terms governing the processing and security of Customer Personal Data under the Agreement.

2. Definitions

2.1 Capitalized terms used but not defined in these Terms have the meanings set out in the Agreement. In these Terms, unless stated otherwise:

- Account has the meaning given in the Agreement or, if no such meaning is given, means Customer's account for the Services.
- Additional Product means a product, service or application provided by Google or a third party that: (a) is not part of the Services; and (b) is accessible for use within the user interface of the Services or is otherwise integrated with the Services.

- 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 and other features and/or functionality of the Services such as logging and monitoring, and identity and access management.
- Admin Console has the meaning given in the Agreement or, if not such meaning is given, means the online console(s) and/or tool(s) provided by Google to Customer for administering the Services.
- Affiliate has the meaning given in the Agreement or, if not such meaning is given, means any entity that directly or indirectly controls, is controlled by, or is under common control with, a party.
- Alternative Transfer Solution means a solution, other than Privacy Shield, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR.
- Audited Services means the Services indicated as being in-scope for the relevant certification or report at https://fabric.io/terms/faq#certifications, as may be updated by Google from time to time.
- Customer Data has the meaning given to "Developer Data" in the Agreement or, if no such meaning is given, means data provided by or on behalf of Customer or Customer End Users via the Services (except TSS and any other support services, if applicable) under the Account.
- Customer End Users has the meaning given to "End Users" in the Agreement or, if no such meaning is given, means the users of Customer's services (for example, the users of a Customer app).
- Customer Personal Data means the personal data contained within the Customer Data.
- 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 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 attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- European Data Protection Legislation means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
- EEA means the European Economic Area.
- 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.

- Google's Third Party Auditor means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.
- Infrastructure Provider has the meaning given in Section 5.4 (Infrastructure Provider).
- Non-European Data Protection Legislation means data protection or privacy legislation in force outside the European Economic Area and Switzerland.
- Notification Email Address means the email address(es) designated by Customer in the Admin Console to receive certain notifications from Google.
- Privacy Shield means the EU-U.S. Privacy Shield legal framework and the Swiss-U.S. Privacy Shield legal framework.
- 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).
- Services has the meaning given to "Services" or "Answers Kit Services" (as applicable) in the Agreement.
- SOC 2 Report means a confidential Service Organization Control (SOC) 2 report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability, as produced by Google's Third Party Auditor in relation to the Audited Services.
- Subprocessors means third parties authorized under these Terms to have logical access to and process Customer Personal Data in order to provide parts of the Services.
- Term means the period from the Terms 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.
- Terms Effective Date means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.
- Third Party Subprocessors has the meaning given in Section 11.1 (Consent to Subprocessor Engagement).

2.2 The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in these Terms have the meanings given in the GDPR.

3. Duration of these Terms

These Terms will take effect on the Terms Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Customer Personal Data by Google as described in these Terms.

4. Scope of Data Protection Legislation

4.1 Application of European Legislation. The parties acknowledge and agree that the European Data Protection Legislation 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; and/or
- the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

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

4.3 Application of Terms. Except to the extent these Terms state otherwise, these Terms will apply irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation 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 the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

- the subject matter and details of the processing are described in Appendix 1;
- Google is a processor of that Customer Personal Data under the European Data Protection Legislation;

- Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Legislation; and
- each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2 Authorization by Third Party Controller. If European Data Protection Legislation applies to the process of Customer Personal Data and Customer is a processor, Customer warrants to Google that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Google as another processor, have been authorized by the relevant controller.

5.1.3 Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

5.2 Scope of Processing.

5.2.1 Customer's Instructions. By entering into these Terms, Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services); (c) as documented in the form of the Agreement, including these 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 Terms.

5.2.2 Google's Compliance with Instructions. Google will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Google is subject requires other processing of Customer Personal Data by Google, in which case Google will inform Customer (unless that law prohibits Google from doing so on important grounds of public interest) via the Notification Email Address.

5.3 Additional Products. If Customer uses an Additional Product, the Services may allow that Additional Product to access Customer Personal Data as required for the interoperation of the Additional Product with the Services. For clarity, these Terms do 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.

5.4 Infrastructure Provider. Customer authorizes the engagement of Amazon Web Services, Inc. ("Infrastructure Provider") to provide underlying infrastructure services in the provision of the Services. Infrastructure Provider's role includes processing Customer Personal Data but Infrastructure Provider will not be a Third Party Subprocessor for the purposes of these Terms.

6. Data Deletion

6.1 Deletion by Customer. Google will enable Customer to delete Customer Personal Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Personal Data during the Term and that Customer Personal Data cannot be recovered by Customer, this use will constitute an instruction to Google to delete the relevant Customer Personal 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 EU or EU Member State law requires storage.

6.2 Deletion on Termination. On expiry of the Term, Customer instructs Google to delete all Customer Personal Data (including existing copies) from Google's systems in accordance with applicable law. Google will, after a recovery period of up to 30 days following such expiry, comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the Term expires, any Customer Personal Data it wishes to retain afterwards.

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 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"). As described in Appendix 2, the Security Measures include measures to encrypt personal data; to help ensure ongoing

confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and 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 Services.

7.1.2 Security Compliance by Google Staff. Google will 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, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3 Additional Security Controls. In addition to the Security Measures, Google will make the Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Personal Data; and (b) provide Customer with information about securing, accessing and using Customer Personal Data.

7.1.4 Google's Security Assistance. Customer agrees that 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 any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

- implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);
- making the Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);
- complying with the terms of Section 7.2 (Data Incidents); and
- providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the Agreement including these Terms.

7.2.Data Incidents

7.2.1 Incident Notification. If Google becomes aware of a Data Incident, Google will: (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Customer Personal Data.

7.2.2 Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Google recommends Customer take to address the Data Incident.

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 Personal Data by Google. Google will not assess the contents of Customer Personal Data to identify information subject to any specific legal requirements. 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(s).

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 Section 7.1 (Google's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

- Customer is solely responsible for its use of the Services, including:
    - making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;
    - securing the account authentication credentials, systems and devices Customer uses to access the Services;
    - backing up its Customer Personal Data; and
- Google has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (for example, offline or on-premise storage), or to protect Customer Personal Data by implementing or maintaining Additional Security Controls except to the extent Customer has opted to use them.

7.3.2 Customer's Security Assessment.

- Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Google's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable.
- Customer acknowledges and agrees that (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) 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 the Customer Personal Data.

7.4 Security Certifications and Reports. Google will update the SOC 2 Report at least once every 18 months in order to evaluate and help ensure the continued effectiveness of the Security Measures.

7.5 Reviews and Audits of Compliance

7.5.1 Reviews of Security Documentation. In addition to the information contained in the Agreement (including these Terms), Google will make available for review by Customer the then-current SOC 2 Report, following a request by Customer in accordance with Section 7.5.3(a), in order to demonstrate compliance by Google with its obligations under these Terms..

7.5.2 Customer's Audit Rights.

- If the European Data Protection Legislation 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 these Terms in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Google will contribute to such audits as described in Section 7.4 (Security Certifications and Reports) and this Section 7.5 (Reviews and Audits of Compliance).
- Customer may also conduct an audit to verify Google's compliance with its obligations under these Terms 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.

- Customer must send any requests for reviews of the SOC 2 Report under Section 7.5.1 or audits under Section 7.5.2(a) or 7.5.2(b) via https://fabric.io/terms/faq#dpo as described in Section 12 (Fabric Data Protection Team; Processing Records).
- 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 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).
- Google may charge a fee (based on Google's reasonable costs) for any review of the SOC 2 Report under Section 7.5.1 and/or 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 review or audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.
- 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.
- Nothing in these 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:
    - any data of any other customer of Google or its Affiliates;
    - Google or its Affiliates' internal accounting or financial information;
    - any trade secret of Google or its Affiliates;
    - any information that, in Google's reasonable opinion, could: (A) compromise the security of any of Google or its Affiliates' systems or premises; or (B) cause Google or its Affiliates to breach obligations under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable, or its security and/or privacy obligations to Customer or any third party; or
    - 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 and/or Non-European Data Protection Legislation, as applicable.

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 any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

- providing the 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); and
- providing the information contained in the Agreement including these Terms.

9. Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Google will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of Customer Personal Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Personal Data.

9.2 Data Subject Requests

9.2.1 Customer's Responsibility for Requests. During the Term, if Google receives any request from a data subject in relation to Customer Personal Data, Google will advise the data subject to submit their request to Customer and 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. Customer agrees that Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

- providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls); and
- complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. Data Transfers

10.1 Data Storage and Processing Facilities. Google may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process the relevant Customer Personal Data anywhere Google or its Subprocessors, or any Infrastructure Provider maintains facilities.

10.2 Transfers of Data Out of the EEA

10.2.1 Google's Transfer Obligations. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data out of the EEA, and the European Data Protection Legislation applies to the transfers of such data, Google will ensure that:

- the parent company of the Google group, Google LLC, remains self-certified under Privacy Shield on behalf of itself and its wholly-owned U.S. subsidiaries; and
- the scope of Google LLC's Privacy Shield certification includes Customer Personal Data.

10.2.2 Customer's Transfer Obligations. If under the European Data Protection Legislation Google reasonably requires Customer to use an Alternative Transfer Solution offered by Google, and reasonably requests that Customer take any action (which may include execution of documents) strictly required to give full effect to such solution, Customer will do so.

11. Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes Google to engage Google's Affiliates as Subprocessors. In addition, Customer generally authorizes Google to engage any other third parties as Subprocessors ("Third Party Subprocessors").

11.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at: https://fabric.io/terms/subprocessors (as may be updated by Google from time to time in accordance with these Terms).

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

- 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 Terms) and Privacy Shield; and
    - if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in these Terms, are imposed on the Subprocessor; and
- remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 Opportunity to Object to Subprocessor Changes.

- When any new Third Party Subprocessor is engaged during the Term, Google will, at least 30 days before the new Third Party Subprocessor processes any Customer Personal Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) either by sending an email to the Notification Email Address or via the Admin Console.
- Customer may object to any new Third Party Subprocessor by terminating the Agreement immediately upon written notice to Google, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. Fabric Data Protection Team; Processing Records

12.1 Google's Representative. Customer may contact a Google representative in relation to the exercise of its rights under these Terms via the methods described at https://fabric.io/terms/faq#dpo (and/or via such other means as Google may provide from time to time).

12.2 Google's Processing Records. Customer acknowledges that Google is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which

Google is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly Customer will, where requested, provide such information to Google via the Admin Console or other means provided by Google, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

13. Liability

13.1 If the Agreement is governed by the laws of:

- a state of the United States of America, then, notwithstanding anything else in the Agreement, the total liability of either party towards the other party under or in connection with these Terms will be limited to the maximum monetary or payment-based amount at which that party's liability is capped under the Agreement (for clarity, any exclusion of indemnification claims from the Agreement's limitation of liability will not apply to indemnification claims under the Agreement relating to the Data Protection Legislation); or
- 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 Terms will be subject to the exclusions and limitations of liability in the Agreement.

14. Effect of these Terms

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between these Terms and the remaining terms of the Agreement, these Terms will govern.

15. Changes to these Terms

15.1 Changes to URLs. From time to time, Google may change any URL referenced in these Terms and the content at any such URL.

15.2 Changes to these Terms. Google may change these Terms if the change:

- is expressly permitted by these Terms, including as described in Section 15.1 (Changes to URLs);
- reflects a change in the name or form of a legal entity;
- is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or
- does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, Google's processing of Customer Personal Data, as described in Section 5.2.2 (Google's Compliance with Instructions); and (iii) otherwise have a material adverse impact on Customer's rights under these Terms, as reasonably determined by Google.

15.3 Notification of Changes. If Google intends to change these 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 Admin Console. If Customer objects to any such change, Customer may terminate the Agreement by giving written notice to Google within 90 days of being informed by Google of the change.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Services to Customer.

Duration of the Processing

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

Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with these Terms.

Categories of Data

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

Appendix 2: Security Measures

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 Services.

1. Data Center and Network Security

This Section 1 describes only Google-owned and operated data center and network security and not those operated by any Infrastructure Provider.

(a) Data Centers.

- Infrastructure. Google maintains geographically distributed 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 diesel generator systems take over. The diesel 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 of products in production environments.
- Businesses 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.

(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 Google-controlled 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. This Section 2(a) describes only Google-owned and operated data center site controls and not those of any Infrastructure Provider.

- 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 an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and

other critical areas. 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 must authenticate themselves via a service-specific authentication system in order to administer 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 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 detect any inappropriate access. Google employs access management systems to control personnel access to production servers for the Services, and only provides access to a limited number of authorized personnel. 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 internal data access policies and training. 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

- Data Storage, Isolation and Logging. Google stores data in a multi-tenant environment on Google-owned or Infrastructure Provider-owned servers. Google also logically isolates the Customer's data. 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 Customer End Users for specific purposes.

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 backgrounds 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.

5. Subprocessor and Infrastructure Provider Security

- Subprocessors. 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 set out

in Section 11.3 (Requirements for Subprocessor Engagement) of these Terms, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

- Infrastructure Provider. Details regarding the Data Center, Network Security, and Site Control security standards of the Infrastructure Provider, including the Infrastructure Provider's SOC 3 Report, are publicly available at https://aws.amazon.com/compliance/soc-faqs/ (as may be modified or updated by the Infrastructure Provider from time to time).