Spectrum Access System (SAS) Data Processing and Security Terms

By accessing or using the SAS, you are agreeing to the Data Protection and Security Terms (the "DPST" or "Terms"), which supplement any other terms to which you are subject, including any applicable Agreement. For purposes of the DPST, we refer to you as "Customer." ~~If there is a conflict between these Terms and an Agreement, the Agreement terms will control for that conflict.~~

1. Introduction

These Terms reflect the parties' agreement with respect to the terms governing the processing and security of your Customer Account Information.

2. Definitions

2.1. Capitalized terms have the following definitions in these Terms:

~~a.~~

a. "Additional Terms for Non-European Data Protection Legislation" means the additional terms referred to in Appendix 3, which reflect the parties' agreement on the terms governing the processing of certain data in connection with certain Non-European Data Protection Legislation.
b. "Alternative Transfer Solution" means a solution, other than the Transfer Solution, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).
c. ~~b.~~ "Citizens Broadband Services Device" or "CBSD" means a device with a radio access point that is certified by the FCC to operate in the Citizens Broadband Radio Services (3.5GHz) band to provide wireless connectivity and data transmission to and from other devices similarly certified by the FCC.
d. ~~c.~~ "Customer Account Information" means information provided by Customer in connection with the registration of CBSDs, which consist of (i) Customer's name, contact information, legal address, mailing address, contact phone number, contact email, account number, and account password; (ii) identification information for CBSDs registered to Customer as prescribed in "Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification"; (iii) identifying information for all groups of CBSDs for

Customer; and (iv) information relating to the priority access licenses (if any) of Customer including identification numbers, boundary information, protection area, CBSD cluster lists, grouping information, and any leases of such priority access licenses

e. ~~d.~~ "Customer Data" means the anonymized and/or aggregated data and metadata Google receives from the Registered CBSDs (i.e., the data FCC regulations governing the use of CBSDs requires) in the course of Customer's use of the Services, excluding any End User Information.

f. "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 Account Information 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 Account Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

g. "EEA" means the European Economic Area.

h. ~~e.~~ "End User" means an individual that Customer permits to use any End User Device that is served by a Registered CBSD.

i. ~~f.~~ "End User Device" means the user equipment, including but not limited to, handsets, dongles, IOT devices, hotspots, smart phones, or tablet devices operated by Customer or by End Users that may establish wireless connectivity with the authorization and under the control of a Registered CBSD.

j. ~~g.~~ "End User Information" means any End User information, data or content, and includes but is not limited to: i) End User billing and usage information, passwords and PINs; ii) End User transmitted or received content information (phone calls, files, emails, texts, pictures, video, other data content), including names, addresses, locations, e-mail addresses, telephone or mobile device numbers, and PINs, and passwords; iii) End User authentication information and any other demographic information, and iv) other information in connection with use of an End User Device on any Registered CBSD or network of Registered CBSDs (excluding any such information in iv) that may qualify as Customer Data). Customer is obligated to keep such End User Information private and secure and will not provide such End User Information to Google.

~~h. 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 Account Information 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 Account Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.~~

~~i.~~

k. "EEA" means the European Economic Area.

l. ~~j.~~ "European Data Protection Legislation" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) ("FDPA").

m. ~~k.~~ "GDPR" means i) 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~~.~~

~~l~~; and ii) the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

n. "Google's Third Party Auditor" means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

o. ~~m.~~ "ISO 27001 Certification" means an ISO/IEC 27001:2013 certification or a comparable certification in relation to the Services.

p. ~~n.~~ "Non-European Data Protection Legislation" means data protection or privacy legislation other than the European Data Protection Legislation.

q. ~~o.~~ "Notification Email Address" means the email address(es) designated by Customer to receive certain notifications from Google.

r. ~~p.~~ "Security Documentation" means all documents and information made available by Google under Section 6.5.1 (Reviews of Security Documentation).

s. ~~q.~~ "Security Measures" has the meaning given in Section 6.1.1 (Google's Security Measures).

t. ~~r.~~ "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 Services.

u. ~~s.~~ "SOC 3 Report" means a Service Organization Control (SOC) 3 report (or a comparable report), as produced by Google's Third Party Auditor in relation to the Services.

~~t.~~

v. "Standard Contractual Clauses" means the European Commission's standard contractual clauses at https://privacy.google.com/businesses/gdprprocessorterms/sccs, which are standard data protection terms for the transfer of personal data to processors established in third countries that do not ensure an adequate level of data protection, as described in Article 46 of the EU GDPR.

w. "Subprocessors" means third parties authorized under these Terms to have logical access to and process Customer Account Information in order to provide parts of the Services.

x. ~~u.~~ "Transfer Solution" means a lawful mechanism to ensure an adequate level of protection for Customer Account Information transferred outside of the EEA to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).

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, in each case irrespective of whether the GDPR, FDPA or Non-European Data Protection Legislation applies.

3. Scope of Data Protection Legislation

3.1 Application of European Legislation. The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Account Information if, for example:

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

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

3.3 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 Account Information.

3.4 Incorporation of Additional Terms for Non-European Data Protection Legislation. The Additional Terms for Non-European Data Protection Legislation supplement these Data Processing Terms.

4. Processing of Data

4.1 Roles and Regulatory Compliance; Authorization.

4.1.1 Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Account Information, the parties acknowledge and agree that:

a. ~~a.~~ the subject matter and details of the processing are described in Appendix 1;
b. ~~b.~~ Google is a processor of that Customer Account Information under the European Data Protection Legislation;
c. ~~c.~~ Customer is a controller or processor, as applicable, of that Customer Account Information under European Data Protection Legislation; and
d. ~~d.~~ each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Account Information.

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

4.2 Scope of Processing.

4.2.1 Customer's Instructions. By entering into these Terms, Customer instructs Google to process Customer Account Information only in accordance with applicable law: (a) to provide and improve the Services; (b) as further specified via Customer's use of the Services; (c) as documented in the form of an 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.

4.2.2 Google's Compliance with Instructions. Google will comply with the instructions described in Section 4.2.1 (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 Account Information by Google, in which case Google will notify Customer (unless that law prohibits Google from doing so on important grounds of public interest).

4.3 Consents. Customer will obtain and maintain any required consents necessary to (i) permit the access, storage, and processing of Customer Account Information by Google, and (ii) permit the access, processing and storage of Customer Account Information provided to Google, in each case for the purpose of providing and improving the Services. Customer agrees that Google may require Customer to provide separate "pass through" terms of service and/or privacy policies to Customer's End Users if Customer is authorized to resell the Services..

5. Data Deletion

5.1 Deletion by Customer. Google may enable Customer to delete Customer Account Information in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Account Information and that Customer Account Information cannot be recovered by Customer, this use will constitute an instruction to Google to delete the relevant Customer Account Information 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 applicable U.S. laws or regulation, EU or EU Member State law requires storage.

5.2 Services Without Deletion Functionality. If the functionality of the Services does not include the option for Customer to delete Customer Account Information, then Google will comply with any reasonable request from Customer to facilitate such deletion, insofar as this is possible taking into account the nature and functionality of the Services, provided that the parties acknowledge that U.S. laws and federal regulations may require storage of certain Customer Account Information and will comply with such applicable laws and regulations. Google may charge a fee (based on Google's reasonable costs) for any data deletion under this Section 5.2. Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such data deletion.

5.3 Deletion on Termination. On expiry or termination of Services, Customer instructs Google to delete all Customer Account Information (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 U.S. law and federal regulations, EU or EU Member State law requires storage.

6. Data Security

6.1 Google's Security Measures, Controls and Assistance.

6.1.1 Google's Security Measures. Google will implement and maintain technical and organizational measures to protect Customer Account Information 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.

6.1.2 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 Account Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.1.3 Google's Security Assistance. Customer agrees that Google will (taking into account the nature of the processing of Customer Account Information 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:

a. ~~a.~~ implementing and maintaining the Security Measures in accordance with Section 6.1.1 (Google's Security Measures);
b. ~~b.~~ complying with the terms of Section 6.2 (Data Incidents); and
c. ~~c.~~ providing Customer with the Security Documentation in accordance with Section 6.5.1 (Reviews of Security Documentation) and the information contained in these Terms.

6.2 Data Incidents~~.~~

6.2.1 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 Account Information.

6.2.2 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.

6.2.3 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.

6.2.4 No Assessment of Customer Account Information by Google. Google will not

assess the contents of Customer Account Information in order 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).

6.2.5 No Acknowledgement of Fault by Google. Google's notification of or response to a Data Incident under this Section 6.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

6.3 Customer's Security Responsibilities and Assessment.

6.3.1 Customer's Security Responsibilities. Customer agrees that, without prejudice to Google's obligations under Section 6.1 (Google's Security Measures, Controls and Assistance) and Section 6.2 (Data Incidents):

a. ~~a.~~ Customer is solely responsible for its use of the Services, including:
    i. ~~i.~~ making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Account Information; and
    ii. ~~ii.~~ securing the account authentication credentials, systems and devices Customer uses to access the Services.
b. ~~b.~~ Google has no obligation to protect Customer Account Information that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (for example, offline or on-premise storage).

6.3.2 Customer's Security Assessment.

a. ~~a.~~ Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and Google's commitments under this Section 6 (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.
b. ~~b.~~ 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 Account Information as well as the risks to individuals) the Security Measures implemented and maintained by Google as set out in Section 6.1.1 (Google's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Account Information.

6.4 Security Certifications and Reports. Google will do the following to evaluate and help ensure the continued effectiveness of the Security Measures:

a. ~~a.~~ obtain, as soon as reasonably practical, and maintain the ISO 27001 Certification; and
b. ~~b.~~ obtain, as soon as reasonably practical, and update the SOC 2 Report and SOC 3 Report at least once every 18 months.

6.5 Reviews and Audits of Compliance~~.~~

6.5.1 Reviews of Security Documentation. In addition to the information contained in an Agreement (including these Terms), Google will once these are available provide Customer the following documents and information to demonstrate compliance by Google with its obligations under these Terms:

a. ~~a.~~ any certificates issued in relation to the ISO 27001 Certification;
b. ~~b.~~ the then-current SOC 3 Report (if available); and
c. ~~c.~~ the then-current SOC 2 Report (if available), following a request by Customer in accordance with Section 6.5.3.

6.5.2 Customer's Audit Rights.

a. ~~a.~~ If the European Data Protection Legislation applies to the processing of Customer Account Information, 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 6.5.3 (Additional Business Terms for Reviews and Audits). Google will contribute to such audits as described in Section 6.4 (Security Certifications and Reports) and this Section 6.5 (Reviews and Audits of Compliance).
b. ~~b.~~ 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).

6.5.3 Additional Business Terms for Reviews and Audits.

a. ~~a.~~ Customer must send any requests for reviews of the SOC 2 Report under Section 6.5.1(c) or audits under Section 6.5.2(a) or 6.5.2(b) to Google's RCS data protection contact as described in Section 11 (RCS Data Protection Contact; Processing Records).
b. ~~b.~~ Following receipt by Google of a request under Section 6.5.3(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 6.5.1(c); and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 6.5.2(a) or 6.5.2(b).

c. ~~c.~~ Google may charge a fee (based on Google's reasonable costs) for any review of the SOC 2 Report under Section 6.5.1(c) and/or audit under Section 6.5.2(a) or 6.5.2(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.

d. ~~d.~~ Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 6.5.2(a) or 6.5.2(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.

e. If the Standard Contractual Clauses apply under Section 9.2 (Transfers of Data), nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Google LLC under the Standard Contractual Clauses

7. 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:

a. ~~a.~~ providing the Security Documentation in accordance with Section 6.5.1 (Reviews of Security Documentation); and

b. ~~b.~~ providing the information contained in an Agreement including these Terms.

8. Data Subject Rights; Data Export

8.1 Access; Rectification; Restricted Processing; Portability. Google will, in a manner consistent with the functionality of the Services and insofar as possible and legally required, enable Customer to access, rectify and restrict processing of Customer Account Information, including via the deletion functionality provided by Google as described in Section 5, and to export Customer Account Information.

8.2 Data Subject Requests~~.~~

8.2.1 Customer's Responsibility for Requests. If Google receives any request from a data subject in relation to Customer Account Information, 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.

8.2.2 Google's Data Subject Request Assistance. Customer agrees that Google will (taking into account the nature of the processing of Customer Account Information and insofar as possible and legally required) 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 complying with the commitments set out in Section 8.1 (Access; Rectification; Restricted Processing; Portability) and Section 8.2.1 (Customer's Responsibility for Requests).

9. Data Transfers

9.1 Data Location ~~and Transfers~~. Customer acknowledges and agrees that the Services may involve the transfer and storage of Customer Account Information outside the EEA. Google may store or process the relevant Customer Account Information anywhere Google or its Subprocessors maintain facilities, provided that Google ensures an adequate level of protection for Customer Account Information by implementing a Transfer Solution. ~~As of the effective date of the Agreement or the date Customer accesses the Services, if there is no Agreement, the parties acknowledge that the Transfer Solution shall be Google LLC adherence to the EU-US Privacy Shield and Swiss to US Privacy Shield frameworks, on behalf of itself and its wholly owned U.S. subsidiaries.~~

~~9.2~~

9.2 Transfers of Data. If the storage and/or processing of Customer Account Information involves transfers of Customer Account Information from the EEA, Switzerland, or the UK to any third country that is not subject to an adequacy decision under the European Data Protection Legislation:

(a) Customer (as data exporter) will be deemed to have entered into the Standard Contractual Clauses with Google LLC (as data importer);

(b) the transfers will be subject to the Standard Contractual Clauses; and

(c) Google will ensure that Google LLC complies with its obligations under such Standard Contractual Clauses regarding such transfers.

9.3 Alternative Transfer Solution. In the event that, an existing Transfer Solution is deemed by a court of competent jurisdiction not to be valid, Google shall adopt an Alternative Transfer Solution, at its discretion. Google will make information available to Customer about its adoption of the Alternative Transfer Solution and ensure that any transfers of Customer Account Information are made in accordance with such Alternative Transfer Solution.

~~9.3~~9.4 Data Center Information. Information about the locations of Google ~~will make~~data centres is available ~~to Customer information about the countries in which data centers used to store Customer Account Information are located~~at www.google.com/about/datacenters/locations/.

10. Subprocessors

10.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Google's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors ("Third Party Subprocessors"). If the Standard Contractual Clauses apply under Section 9.2 (Transfers of Data), the above authorizations constitute Customer's prior written consent to the subcontracting by Google LLC of the processing of Customer Account Information.

10.2 Information about Subprocessors. At the written request of the Customer, Google will provide information regarding Subprocessors and their locations. Any such requests must be sent to Google using the contact details set out in Section 11.1 (Data Protection Contact for Google).

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

a. ~~a.~~ ensure via a written contract that:
   i. ~~i.~~ the Subprocessor only accesses and uses Customer Account Information to the extent required to perform the obligations subcontracted to it, and does so in accordance with an Agreement (including these Terms) and Alternative Transfer Solution adopted by Google as described in Section 9 (Data Transfers); and
   ii. ~~ii.~~ if the GDPR applies to the processing of Customer Account Information, the data protection obligations set out in Article 28(3) of the GDPR, as

described in these Terms, are imposed on the Subprocessor; and

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

10.4 Opportunity to Object to Subprocessor Changes.

a. ~~a.~~ 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 Account Information, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

b. ~~b.~~ 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 10.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

11. SAS Data Protection Contact; Processing Records

11.1 Google's SAS Data Protection Contact. Google's SAS data protection contact can be reached via email to ~~sas-support@google.com~~sas-support@google.com (and/or via such other means as Google may provide from time to time).

11.2 Google's Processing Records. Customer acknowledges that Google is required under the GDPR, in addition to any requirements under other applicable laws, 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, if the GDPR applies to the processing of Customer Account Information, Customer will, where requested, provide such information to Google and ensure that all information provided is kept accurate and up-to-date.

12. Limitation of Liability

Unless otherwise addressed in an Agreement, the maximum monetary or amount at which each party's liability is capped under the DPST is the amount you paid for

the SAS Services during the twelve months prior to the event giving rise to the liability, whichever is greater.

13. Third Party Beneficiary

Google LLC will be a third party beneficiary of Section 6.5 (Reviews and Audits of Compliance), and Section 10.1 (Consent to Subprocessor Engagement) of these Terms.

14. Modification

Google may modify these Terms i) to reflect changes to the law, or ii) changes to our SAS Services or data protection or security practices, provided that such change will not have a material adverse impact on Customer's rights hereunder. You should look at the these Terms regularly; Google will post notice of modifications to these Terms. Changes will not apply retroactively and will become effective no sooner than 30 days after they are posted. However, changes made for legal reasons (including changes required by the FCC and WInnForum) will be effective immediately. If you do not agree to the modified Terms, you should discontinue your use of the Services. Your continued use of the Services constitutes your acceptance of the modified Terms.

15. Effect of this Data Processing Addendum

If there is any conflict or inconsistency between the Standard Contractual Clauses, the Additional Terms for Non-European Data Protection Legislation, this Data Processing Addendum, and the remainder of the Agreement, then the following order of precedence will apply:

(a) the Standard Contractual Clauses;

(b) the Additional Terms for Non-European Data Protection Legislation;

(c) the remainder of these Terms; and

(d) the remainder of the Agreement.

If this Agreement (including any Addendum) is translated into any other language, and the translated text conflicts or is inconsistent with the English text, the English text will govern.

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

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 effective date of an applicable Agreement or the date Customer accesses the Services, if there is no Agreement, plus the period from the expiry or termination of the Services until deletion of all Customer Account Information by Google in accordance with the Terms.

Nature and Purpose of the Processing

Google will process Customer Account Information for the purposes of providing and improving the Services to Customer in accordance with the Terms.

Categories of Data

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

Data Subjects

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

Appendix 2: Security Measures

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. Solely purposes of this Appendix 2, "Google" refers to Google and its

Affiliates.

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 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 an operating system 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.

Business Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Data centers are typically connected via high-speed private networks 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. ~~1.~~ tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. ~~2.~~ employing intelligent detection controls at data entry points; and
3. ~~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 use of HTTPS encryption (also referred to as SSL or TLS connection). Google servers may use ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA. 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 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 central authentication system or via a single sign on 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 a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards may include password expiry, 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.

(b) Decommissioned Disks and Disk Erase Policy. Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "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

Customer'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 Account Information are required to complete additional requirements appropriate to their role (eg., certifications). Google's personnel will not process Customer Account Information 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 set out in Section 10.3 (Requirements for Subprocessor Engagement) of these Terms, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 3: Additional Terms for Non-European Data Protection Legislation

The following Additional Terms for Non-European Data Protection Legislation supplement these Data Processing Terms:

CCPA Service Provider Addendum to Spectrum Access System (SAS) Data Processing and Security Terms

This CCPA Service Provider Addendum to the Spectrum Access System (SAS) Data Processing and Security Terms (the "CCPA Addendum") is entered into by Google and the Customer and also supplements the Agreement.

1. Introduction

This CCPA Addendum reflects the parties' agreement on the processing of Customer Personal Information in connection with the California Consumer Privacy Act of 2018

("CCPA"). This CCPA Addendum is effective solely to the extent the CCPA applies.

2. Definitions and Interpretation

2.1 The terms "business purpose", "personal information", "sale", and "service provider" as used in this CCPA Addendum have the meanings given in the CCPA.

2.2 "Customer Personal Information" means personal information that is processed by Google on behalf of Customer in Google's provision of the Services.

2.3 Capitalised terms used but not defined in this CCPA Addendum will have the meanings given in the DPA.

2.4 If this CCPA Addendum conflicts or is inconsistent with the remainder of the Agreement (including the DPA), this CCPA Addendum will govern.

3. Service Provider

3.1 Google may offer and Customer may use certain services in which Google acts as a "service provider" as defined under the CCPA. Subject to the terms of this CCPA Addendum and solely with respect to such services, Google will act as Customer's service provider, and as such, will not retain, use, or disclose Customer Personal Information, other than (a) for a business purpose under the CCPA on behalf of Customer and the specific purpose of performing the Services, or (b) as otherwise permitted under the CCPA, including any applicable exemption from "sale" in the CCPA, as reasonably determined by Google.

3.2 Customer is solely liable for its compliance with the CCPA in its use of Google services.

4. Changes to this CCPA Addendum.

In addition to Section 14 of the Terms (Modifications), Google may change this CCPA Addendum without notice if the change (a) is based on applicable law, applicable regulation, a court order, or guidance issued by a governmental regulator or agency; and

(b) does not have a material adverse impact on Customer with respect to exemptions from “sales” under the CCPA, as reasonably determined by Google.