VIASAT TRUSTED CYBERSECURITY SERVICE
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") applies to the Processing of Personal Data by Viasat, Inc. ("**Viasat**") under either the Trusted Cybersecurity Service Pilot Program Agreement or the Master Services Agreement (each, an "**Agreement**") applicable to Viasat's Cybersecurity Services (the "**Services**").

1. **Definitions.** The following terms shall have the meanings ascribed to them in this Section. Capitalized terms used in this Addendum that are not defined herein shall have the same meaning as set forth in the Agreement.

   "Common Broadcast Incidents" means, without limitation, pings and other broadcast attacks on a party's firewall or any software or service infrastructure used for the Services, port scans and unsuccessful log-on attempts so long as such incidents do not need to be reported to a supervisory authority under Data Protection Laws and are: (i) routine occurrences, (ii) not objectively determined to be specifically targeted at the Services, and (iii) no such incident results in unauthorized access, use, disclosure, modification or destruction of Personal Data or intentional interference with system operations in an information system that contains Personal Data.

   "Controller" means the party that alone or jointly with others determines the purpose and means of the Processing of Personal Data.

   "Data Breach" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data caused by Viasat.

   "Data Protection Laws" means, as and to the extent they apply to a party, any applicable laws, rules, or regulations that relate to the privacy or Processing of Personal Data of Data Subjects, including without limitation: (a) United States federal law, (b) state laws, including the California Consumer Privacy Act, Colorado Privacy Act, and Virginia Consumer Data Protection Act, (c) EEA/UK Data Protection Law, (d) Brazil Laws No. 13,709/2018 (General Law for the Protection of Personal Data or "LGPD") and No. 12,965/2014 (Internet Law), and (e) any other similar applicable laws or regulations that are in effect or come into effect during the term of the Agreement.

   "Data Subject" means an identified or identifiable natural person, including such persons set out in **Schedule 1**.

   "EEA" means the European Economic Area.

   "EEA/UK Data Protection Law" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

   "Good Industry Practice" means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.

   "Personal Data" means any information contained within Client Data that relates to a Data Subject, and includes information referred to as personally identifiable information, personal information, or similar terms as may be defined within the Data Protection Laws.

"Processor" means the party that Processes Personal Data on behalf of the Controller.

"Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where Data Protection Laws that affect transfers other than those in (i) and (ii) herein apply, transfers involving jurisdictions as may be described in **Schedule 4**.

"Standard Contractual Clauses" or **"SCC"** means (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"); and (iii) where Data Protection Laws of other jurisdictions apply, the contractual clauses as described in **Schedule 4**.

"Subprocessors" means Viasat's subcontractors approved by Client, who Viasat engages in the Processing of Personal Data; as of the Effective Date, such subcontractors are listed in **Schedule 3**.

The terms "**transfer**", "**supervisory authority**", "**data protection impact assessment**", "**special categories of Personal Data**" and "**appropriate technical and organizational measures**" shall be interpreted in accordance with the Data Protection Laws. Words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in the Data Protection Laws.

2. Personal Data Processing

a. **Compliance with Law**. Each party shall comply with Data Protection Laws when Processing Personal Data, and shall not cause the other party to violate the Data Protection Laws in their respective roles under this Addendum.

b. **Personal Data Processed by Client in the Services.** Unless otherwise agreed to in writing by the Parties, Client shall operate as a Controller with respect to Personal Data and shall have sole responsibility for the accuracy, quality, and legality of such Personal Data and the means by which Client acquires and Processes Personal Data. Client's instructions for the Processing of Personal Data by Viasat in its capacity as a Processor shall comply with the Data Protection Laws.

3. Viasat as Data Processor

a. **Details of the Processing.** Viasat will Process Personal Data based on Client's instructions, which shall include the Agreement and this Addendum (including as described in Schedule 1). For the avoidance of doubt, Viasat shall not: (i) sell Personal Data; (ii) Process Personal Data for any purpose other than for the purposes specified in the Agreement; (iii) Process the Personal Data outside the direct business relationship with Client; or (iv) combine Personal Data with data relating to identified or identifiable individuals that Viasat receives from, or on behalf of, another person or persons, or collects from its own interactions with Data Subjects unless such combining of data is expressly permitted by and carried out in accordance with the Data Protection Laws. If Viasat must process Personal Data as otherwise required by the Data Protection Laws, Viasat shall inform Client of such legal requirement before Processing the Personal Data, unless that Data Protection Law prohibits such disclosure on important grounds of public interest. In addition, Viasat will immediately inform Client if, in its opinion, an instruction from Client infringes the Data Protection Laws.

b. **Security.** Viasat shall apply reasonable and appropriate technical and organizational measures to the Services to ensure the confidentiality, availability and integrity of Personal Data. The minimum technical and organizational measures to be implemented by Viasat for the Services are set forth in Schedule 2. Viasat shall ensure that persons authorized to carry out Processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality. Viasat shall preserve Personal Data in accordance with Client's reasonable instructions and requests, including any retention schedules and/or litigation hold orders provided by Client to Viasat, where such instructions and requests do not materially conflict with Viasat's data retention policies and procedures.

c. **Breach Management and Notification.** Viasat shall maintain reasonable and appropriate security incident management policies and procedures for responding to a Data Breach. In the event of a Data Breach, Viasat shall: (a) provide notice to Client without undue delay after having become aware of a Data Breach; (b) use commercially reasonable efforts and take all necessary actions to contain, remediate the cause of, and mitigate the impact of the Data Breach; (c) collect, preserve, and document all evidence concerning the discovery, cause, vulnerability, remedial actions, and impacts related to such Data Breach and provide this information to Client upon request; and (d) cooperate with Client and its designees for purposes of Data Breach response, including any notice by Client. Unless Viasat is instructed by an applicable governmental authority to notify a third party of a Data Breach, a decision to notify a third party of a Data Breach shall be in Client's sole discretion. The provision of Data Breach notifications to any individuals, third parties, or governmental authorities, including the content, shall be at the reasonable discretion and reasonable direction of Client. For the sake of clarity, the obligations in this section shall not apply to Common Broadcast Incidents.

d. **Requests and Assistance**. Viasat shall, to the extent legally permitted, promptly notify Client if Viasat receives a request from a Data Subject to exercise her/his rights under Data Protection Laws or receives a request or complaint from a supervisory authority or other third party ("**Request**"). Taking into account the nature of the Processing, Viasat shall assist Client in the fulfilment of Client's obligation to respond to the Request, and shall not respond to the Request without written instructions and approval from Client. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Request, Viasat shall upon Client's written request use commercially reasonable efforts to assist Client in responding to such Request, to the extent Viasat is legally permitted to do so. Upon request by Client, Viasat shall assist Client as necessary and required to carry out data protection impact assessments related to Client's use of the Services, and in the cooperation or prior consultation with supervisory authorities in the performance of Viasat's tasks relating to the data protection impact assessments.

e. **Subprocessors**. Viasat shall not disclose or otherwise make available Personal Data to any third party (other than the applicable Data Subject) unless Viasat: (i) notifies Client of the anticipated disclosure at least ten (10) days in advance of such planned disclosure (so as to provide Client the opportunity to oppose the disclosure based on reasonable grounds relating to data protection and obtain a protective order or seek other relief); and (ii) contractually imposes upon the third party data privacy and security obligations that are materially no less protective than those in the Agreement. Client provides specific written authorization for Viasat's use of the Subprocessors identified in **Schedule 3**. Viasat shall be liable for the acts and omissions of its Subprocessors to the same extent it would be liable if performing the services of each subprocessor directly under the terms of the Agreement.

f. **Notice of New Subprocessors.** Viasat shall notify Client of its intent to disclose Personal Data to a new subprocessor according to the "Subprocessors" section above in compliance with any Notice provisions in the Agreement.

g. **Personal Data Transfers**

i. ***Restricted Transfers***. The Parties agree that the transfers permitted under the Agreement are limited to those described in Schedule 1. Transfers of Personal Data that are Restricted Transfers shall be subject to the appropriate Standard Contractual Clauses or other terms as described in Schedule 4. If any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

ii. ***Onward Transfers***. Viasat shall not participate in (nor permit any Subprocessor to participate in) any other Restricted Transfers of Personal Data (whether as an exporter or an importer of the Personal Data) unless the Restricted Transfer is made in compliance with the Data Protection Laws and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Personal Data or where the importer has adopted an alternative transfer mechanism that complies with the Data Protection Laws.

h. **Audit**. Not more than once a year, and in order to assess compliance with the data protection provisions herein, upon Client's request, Viasat will furnish to Client a certification or attestation from an accredited third-party (*e.g.*, ISO 27001, ISO 27017-27018, SOC Type II, etc.) (an "**Accredited Certification**") relating to the results of an audit of the systems applicable to the Services (or if (i) such certification or attestation is unavailable, (ii) such certification or attestation does not cover the specific scope in question, or (iii) Viasat experiences a Data Breach in relation to the Services), Client may submit to Viasat a written security questionnaire requesting a written description of the technical and organizational measures employed by Viasat. Viasat shall reply within 30 days of receipt of the request, or as otherwise agreed to by the Parties. If, based on Viasat's responses to the third-party certification or attestation, or questionnaire, Client reasonably believes that an on-site audit is necessary for compliance with data protection obligations set forth in this Addendum, Client may request that either it, or a third party, conducts an audit pursuant to the following conditions:

i. an audit plan must be agreed to by both Parties 30 days in advance of the proposed audit date together with any third-party auditor performing the audit; the audit plan will describe the scope, duration, third-party auditor and start date of the audit, and shall take into consideration Viasat's confidentiality and security obligations towards its customers and employees as well as the scope of any previously provided Accredited Certification;

ii. the audit will be limited to the systems that Process Personal Data in relation to the Services;

iii. audits must be conducted during regular business hours, according to Viasat's policies so as not to interfere with Viasat's business activities;

iv. where Client uses a third-party auditor, audits may be performed only if a confidentiality agreement is concluded with the auditor and the audit results will remain confidential and will not be shared with third parties unless agreed by the Viasat;

v. Client must provide Viasat with any audit report generated in connection with any audit pursuant to this Agreement at no charge, unless otherwise stated in the applicable Laws;

vi. audits are performed at Client's expense and Viasat will cooperate and assist in the performance of the audit plan; and

vii. the parties will confer regarding any findings from such audits and develop a reasonable timeline and plan for remediation of such findings, and Viasat shall remediate such findings.

i. **Jurisdiction Specific Terms**. Schedule 4 contains terms that, in addition to the terms set forth in the main body of this Addendum, apply to the Processing and transfer of Personal Data according to jurisdiction-specific Data Protection Laws. In the event of any conflict between such jurisdiction-specific terms and the main section of this Addendum, the jurisdiction-specific terms shall control.

j. **Return and Destruction**. Viasat shall return or destroy all Personal Data (such that the Personal Data is rendered unusable and unreadable, or is maintained only in Anonymized form) in accordance with the terms in the Agreement governing the return or destruction of Client Data upon termination or expiration of the Agreement. Upon written request of Client, Viasat shall provide written certification that all such Personal Data has been returned or deleted.

k. **Notices**. Notices required or permitted to be given to Viasat herein shall be provided to Vendor's primary point of contact at Viasat, or as otherwise described in the Agreement, and by email to privacy@viasat.com.

l. **Indemnification and Liability**. The applicable indemnification and liability terms in the Agreement shall apply to each party's obligations in this Addendum.

m. **Effect of These Addendum Terms**. Except as otherwise set forth herein and in the Agreement, the terms and conditions of this Addendum, including its Schedules, are part of and incorporated into the Agreement, and the terms and conditions of this Addendum constitute the entire and exclusive agreement between the parties with respect to its subject matter. To the extent of any conflict or inconsistency between this Addendum and the terms of the Agreement, this Addendum will govern. The parties agree to cooperate in good faith to amend these terms and/or enter into additional terms as necessary to address modifications, amendments, or updates to the Data Protection Laws.

Schedule 1

Description of Personal Data Processing and Transfer

Categories of Data Subjects whose Personal Data is Processed:	Client personnel
Categories of Personal Data Processed:	Device IP address; Personal Data as determined by Client
Sensitive or special categories of Personal Data Processed (if applicable):	As determined by Client
Location(s) to which Personal Data is transferred as part of Processing:	United States
Frequency of any transfer, *e.g.*, whether the Personal Data is transferred on a one-off or continuous basis:	Continuous
Nature of the Personal Data Processing, *e.g.*, collection, storage, alteration, etc.:	Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction, erasure or destruction.
Purpose(s) of the Personal Data transfer and further Processing:	Personal Data shall be Processed to perfom the Services, and fulfill the terms of the Agreement and this Addendum, including: • Regulatory and law enforcement compliance, • Delivery and support of services to the Client, and • Analytics relating to services to the Client. **Form of Processing:** electronic
Duration for which the Personal Data will be retained, or, if unclear, the criteria used to determine that period:	2 weeks

Schedule 2

Minimum Technical and Organization Measures

General

Viasat has implemented and shall maintain commercially reasonable and appropriate technical and organizational measures consistent with Good Industry Practices to ensure the confidentiality, integrity, and availability of Personal Data, including where appropriate the policies, and procedures and internal controls set forth in this **Schedule 2**.

Access Control of Processing Areas

Viasat shall implement commercially reasonable and appropriate measures in order to prevent unauthorized persons from gaining access to the Processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data is Processed, including:

- establishing security areas and physical controls;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective and documentation;
- Logging, monitoring, and tracking all access to the data center where Personal Data is hosted.

Access Control to Data Processing Systems

Viasat shall implement commercially reasonable and appropriate measures to prevent Processing systems, where Personal Data is Processed, from being used by unauthorized persons, including:

- use of industry standard encryption technologies, including for data at rest and in-transit;
- use of multifactor authentication for remote access;
- identification of the terminal and/or the terminal user to Viasat and processing systems;
- automatic temporary lock-out of user terminal if left idle with identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- Logging, monitoring, and tracking of all access to data content.

Access Control to Use Specific Areas of Data Processing Systems

Viasat commits that the persons entitled to use its Processing system are only able to access the Client Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;

- use of industry standard encryption technologies, including for data at rest and in-transit; and
- control of controlled files and documented destruction of data in a timely manner, including as stated in the Agreement.

Availability Control

Viasat shall implement commercially reasonable and appropriate measures to ensure that Personal Data is protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- storage of backup at an alternative site that is available for restore in case of failure of the primary system.

Transmission Control

Viasat shall implement commercially reasonable and appropriate measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This shall be accomplished by various measures including:

- use of industry standard firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- encryption of Personal Data in transit;
- providing user alert upon incomplete transfer of data (end to end check); and
- Logging, monitoring, and tracking of all data transmissions as far as commercially reasonable.

Input Control

Viasat shall implement commercially reasonable and appropriate input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of strong, unique authentication credentials or codes (passwords);
- automatic log-off of user ID's that have not been used for no more than 24 hours; and
- proof established within Viasat's organization of the input authorization; and
- electronic recording of entries.

Documentation

Viasat shall keep documentation of technical and organizational measures in case of audits and for the conservation of evidence in accordance with applicable Law. Viasat shall ensure that persons that it employs, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this **Schedule 2**.

Monitoring

Viasat shall implement commercially reasonable and appropriate measures to monitor access restrictions to Viasat's system administrators and to ensure that they act in accordance with instructions received. This shall be accomplished by various measures including:

- individual appointment of system administrators;
- adoption of commercially reasonable and appropriate measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least one year;
- yearly audits of system administrators' access to assess compliance with assigned tasks, the instructions received by Viasat and the Data Protection Laws.

Schedule 3

Subprocessors

Client has approved the use of the following Subprocessors to Process Personal Data as of the effective date of the Agreement:

- Amazon Web Services (AWS)

Schedule 4

Jurisdiction Specific Terms

The following additional terms apply to the Processing of Client Personal Data in the listed jurisdictions:

Brazil	1. Viasat agrees and undertakes to fully comply with the principles, the Data Subjects rights, and the legal regime established by Brazil's LGPD with regard to the Personal Data subject to Brazilian laws. 2. Viasat represents and warrants to Client that any internal existing data processing policy applicable to the Processing does not conflict with Brazilian laws. 3. The Parties agree to amend the Addendum and adopt SCCs for Restricted Transfers, once these clauses are approved by Brazil's data protection domestic authority and provided that the SCCs are compatible with this Addendum.
California (U.S.)	1. Each of the Parties shall comply with the CCPA, as amended, including by the California Privacy Rights Act ("CPRA") (herein referred to as the "California Privacy Laws"), with Client in the capacity of a "Business" and Viasat as a "Service Provider" to Client. 2. Viasat shall not "sell" or "share" the Personal Data (as "sell" and "share" are defined in the California Privacy Laws). 3. Viasat shall provide the level of privacy protection as required by the California Privacy Laws. 4. Within Viasat's contracts with its Subprocessors, Subprocessors shall be "Service Providers" and not "Third Parties" as such terms are defined in the California Privacy Laws.
European Economic Area	1. For Personal Data protected by the EU GDPR that is subject to a Restricted Transfer, the EU SCCs will apply completed as follows: a. Module Two will apply; b. Clause 7 – the optional docking clause will apply; c. Clause 9, Option 2 will apply, and the duration for prior notice of Subprocessor changes shall be as set out in this Addendum; d. Clause 11 – the optional language will <u>not</u> apply; e. Clause 17, Option 1 will apply, and the EU SCCs will be governed by Republic of Ireland law; f. Clause 18(b) – disputes shall be resolved before the courts of Republic of Ireland; g. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1; h. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2. 2. The competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs) is the Irish data protection authority 3. In the event that any provision of this Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

Switzerland	In case of any transfer of Personal Data from Switzerland subject exclusively to the Data Laws of Switzerland ("**Swiss Data Protection Laws**"), (i) general and specific references in the EU SCCs to GDPR or EU or member state law shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the EU SCCs determined by the member state in which the data exporter or Data Subject is established shall refer to an obligation under Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.
United Kingdom	In relation to Personal Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows: (i) The EU SCCs, completed as set out above in this Appendix IV of this Agreement shall also apply to transfers of such Personal Data, subject to sub-clause (ii) below; (ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Agreement.