AMENDED AND RESTATED SWISS REMOTE IDENTIFICATION MASTER AGREEMENT

Version 2.0: 02.12.2021

This Amended and Restated Swiss Remote Identification Master Agreement (the "Agreement") is made by and between the signatory parties listed on the signature page (each, a "Party" and collectively the "Parties") on the date indicated therein.

WHEREAS:

1. Pursuant to a memorandum of cooperation (the "MoC"), the Parties are members of Swiss U-Space Implementation ("SUSI"), a nation-wide collaborative effort developed in Switzerland for the safe integration of drones, otherwise known as "unmanned aerial vehicles/systems" ("drones", "UAVs" or "UAS");

2. One of the focuses of SUSI is the implementation of remote identification of UAS ("RID");

3. RID is subject to Standard 3411-19 issued by ASTM (the "Standard");

The Parties desire to participate in the national implementation of RID and the Standard in Switzerland ("Swiss RID Implementation – "SRID"), in their different capacities, as detailed in the "role" section on the signature page;

5. The Parties are parties to that certain original Master Agreement relating to the subject matter of this Agreement ("Original Agreement").

6. The Parties now intend to amend and restate the Original Agreement with this Agreement, including by adding and executing the attached Standard Contractual Clauses.

THEREFORE, the Parties have agreed their Services (as defined below) within the SRID to be governed by the terms and conditions in this Agreement.

1. DEFINITIONS

1.1. The following definitions shall apply to this Agreement:

"FOCA" means the Swiss Federal Office of Civil Aviation.

"MoC" means the Memorandum of Cooperation signed between SUSI members, as such may be amended from time to time;

"NDA" means the Mutual Non-Disclosure Agreement signed between SUSI members, as such may be amended from time to time.

"Services" shall mean any of the services provided by a Party pursuant to the Agreement.

"Service Provider" means a Party providing a specific Service; for the avoidance of any doubt, Service Provider shall refer herein to a Party providing one or more Services, such as NET-RID service provider, NET-RID display provider or DSS provider.

"SRID Governance rules" shall mean the set of rules governing the functioning and the decision-making process within the SRID, as such may be amended from time to time as outlined in such rules.

“Technical Annex” shall mean any and all annexes hereto with a technical content or managed by the Technical Board, as such annex is designated in its name.

“Technical Board” shall mean the group formed by SUSI members handling all technical aspects related to the SRID, as such aspects may be amended from time to time in accordance with the SRID Governance rules.

“Technical Dispute Resolution Board” shall mean a board formed of 3 (three) members, elected by the Technical Board in accordance with the SRID Governance rules, in charge with the resolution of disputes arising from or in connection with the SRID or this Agreement.

The capitalized terms not defined herein shall have the meaning assigned to them in the Standard, to which extent each Party hereby declares it has acquired a copy thereof.

1.2. For the purposes hereto, the applicable time convention will be CET (Central European Time).

2. SCOPE

2.1. This Agreement governs the rights and obligations of the Parties when providing the Services. Each Party will perform its Services in accordance with the Standard. The Parties hereby fully understand that RID has public acceptance and law enforcement purpose and can be potentially used to enhance situational awareness, but it is not meant as a tool for deconfliction or detect-and-avoid actions.

2.2. In particular, this Agreement defines the indicators associated with the Services, acceptable and unacceptable Service levels, parameters for data sharing between the Parties, dispute resolution procedures for the Parties with respect to the Services and actions to be taken in specific circumstances.

2.3. The objectives of this Agreement are to:

(i) provide clear reference to service ownership, accountability, roles or responsibilities.

(ii) present a clear, concise and measurable description of service management.

(iii) match perceptions of expected service provision with actual service support & delivery.

3. CONDITION

3.1. This Agreement becomes effective for and binding upon each Party on the date of its signature by that Party (“Effective Date”). A preliminary draft of the Technical Annexes is attached hereto. The Technical Board shall: (a) finalize and approve the SRID Governance rules and any and all amendments to the Technical Annexes hereto, as such may be developed during the approval phase; and (b) deliver a copy of the approved Technical Annexes and SRID Governance rules to all Parties. Upon approval by the Technical Board, the SRID Governance rules and the amendments to the Technical Annexes are hereby incorporated by reference into this Agreement. For the avoidance of any doubt, the main body of this Agreement and Annex D Data Sharing Agreement, are hereby considered final and are not subject to the Technical Board approval process.

3.2. It is hereby understood and agreed that this Agreement will automatically terminate for such a Party that notifies the other Parties that it does not accept the Technical Annexes and SRID Governance rules, as such are finalized and approved by the Technical Board in accordance with the process outlined in clause 3.1 above, within ten (10) calendar days of its receipt thereof. If a Party does not provide notice of its rejection of such documents during this period, then it will be deemed to have accepted them.

4. SERVICE MANAGEMENT AND PERFORMANCE

4.1. Service Management.

4.1.1. Service Availability. The Parties will cooperate to reasonably provide the following:

(i) Telephone support, e.g., notice of Service disruption/malfunctioning; availability to be provided as per the time frames indicated in Clause 4.1.2. below;

(ii) Remote assistance, e.g., guidance from one Party to the other;

(iii) Response, e.g., actual intervention of the Service Provider to remedy the cause of the disruption/malfunctioning of the Service, on the software or hardware, as the case may be;

(iv) Security, as per Annex D (Data Sharing Agreement); and

(v) Delivery times for critical information.

4.1.2. Service Requests. In support of Services, each Service Provider will respond to Service-related incidents or requests submitted by another Party in compliance with the below:

Severity Level	Step 1 - Immediate Response (Identify)	Step 2 - Triage (Temporary Fix)		Step 3 - Problem Resolution (Fix)	
	Action / Target Response Time	Action	Target Response Time	Action	Target Response Time
Severity 1 (Critical)	Point of contact acknowledges & 100 % escalation for triage within response 1h	Immediate and continuing best efforts	Next business day	Immediate and continuing best efforts	Update every week and upon request
Severity 2 (Degraded)	Point of contact acknowledges / within 8 hours	Rollback of offending change	2 days	High priority resolution by the engineering team	Updates every 2 days to stakeholders
		Interim fix within 4 days, as agreed with stakeholders	4 days		
Severity 3 (Minimal)	Point of contact acknowledges / within 3 days	Worked on a time available basis	7 days	As appropriate	Update within 15 days

Problem Classification Table

Severity Level	Criteria
Severity 1 (Critical)	The Service(s) of a Service Provider are/is non-operative, significantly impaired or its failures are significantly impacting other Service Providers. No known work around is currently available.
Severity 2 (Degraded)	The Service(s) of a Service Provider do(es) not function as designed, with partial or limited loss of functionality, but a workaround is available.
Severity 3 (Minimal)	This group includes problems that have little or no impact on daily business processes.

4.2. Service Performance.

4.2.1. Service Levels. Each of the Services shall be provided in accordance with the criteria and levels defined herein and will be measured in accordance with Technical Annex B and in any case at least at the levels defined in accordance with the Standard.

4.2.2. Limitations: **Unless otherwise listed in this Agreement, the Services provided by a Party are provided "as is," with all faults, defects, bugs, and errors. Other than the express warranties in this Agreement, each Party disclaims all other warranties of any kind, either express or implied, including implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. While each Party will use reasonable good faith efforts to perform its Services in accordance with the requirements of this Agreement, no Party will be liable to any other Party under this Agreement for any direct, indirect, consequential, incidental, or other damages arising from or in relation to this Agreement or its performance hereunder.**

4.2.3. Exclusions. The following items are excluded from this Agreement:

(i) Temporary down time, such as for upgrades or for routine, regularly scheduled maintenance limited to specified time periods.

(ii) Down time to address emergencies or circumstances outside the Service Provider’s control, such as a widespread power/connectivity failure.

4.3. Testing and Monitoring. Testing and monitoring of the Services will be made as detailed in Technical Annex B.

5. MANAGEMENT ELEMENTS

5.1. Dispute Resolution. The Parties shall use reasonable efforts to resolve disputes amicably. Any disputes that cannot be resolved amicably shall be decided by the Technical Dispute Resolution Board in accordance with the SRID Governance rules.

5.2. Escalation Procedures. Each Party will use all reasonable endeavors to ensure that responses and remedies are provided within the specified timescales detailed in clause 4.1.2. In the event that Service-related incidents or requests submitted by another Party remain outstanding beyond the agreed times, the Technical Contact within the Party receiving such request will escalate the call to the overall contact of the respective Party (as specified in Annex E), who will contact the counterpart within the claiming Party to agree a course of action to be taken.

5.3. SLA Lifecycle: The SLA Lifecycle will be governed by Technical Annex C hereto.

5.4. Decision Making: Any decision to be made by the Parties with respect to this Agreement will be made in accordance with the SRID Governance rules.

5.5. Points of Contact. The following points of contact for execution of and receipt of notices under this Agreement are as listed in Technical Annex E, attached hereto. Each Party may update its point of contact any time by submitting written notice to all other Parties' points of contact.

5.6. Language. All meetings, communications, reports and other activities of the Parties pursuant to this Agreement shall be in English.

5.7. End User Agreements. Each Party will cause end users ("End Users") of any of its products or services that utilize Services provided by any other Party under this Agreement ("End User Services") to enter into a legally binding agreement with it that contains the obligations and restrictions set forth in Annex F. Each Party will provide a copy of such end user agreement to any other Party upon request.

6. DATA SHARING, SECURITY AND MANAGEMENT

Each Party hereby expressly agrees to the terms and conditions of the data sharing agreement in Annex D ("Data Sharing Agreement") which outlines the framework for the sharing of personal information when one Party discloses personal information to the other and the associated responsibilities.

7. REPRESENTATIONS AND WARRANTIES

7.1. Representations and Warranties. Each Party represents and warrants to the other Parties the following: (a) the Party is incorporated and exists under the laws of the jurisdictions of its respective incorporation; (b) the Party has the authority and capacity to enter into this Agreement; (c) the Party has duly executed and delivered this Agreement; (d) this Agreement constitutes a legal, valid and binding obligation, enforceable against the Party in accordance with its terms; and (e) in connection with the Party's performance of its obligations under this Agreement it will not breach any agreement with any third party to which it is bound.

8. COMMUNICATION

8.1. To the extent permitted by the SUSI MoC, each Party is entitled to issue press releases and to make other similar public announcements with respect to the SRID. The Parties will cooperate to draft any common press releases and other public announcements relating to the subject matter of this Agreement and the relationship between the Parties, it being understood that in any case each Party shall be in charge of its own communication efforts related to its participation in the SRID.

8.2. No Party shall use another Party's name, trademarks, service marks, trade names, logos, domain names, or other indicia of source, association, or sponsorship, without the prior written consent of the other Party, which consent shall not be unreasonably withheld.

9. TERM AND TERMINATION

9.1. This Agreement will be effective in accordance with Clause 2 above and shall continue to be effective for as long as the Parties participate in the SRID.

9.2. The Agreement may only be terminated by mutual agreement of all current Parties to the Agreement. An individual Party's status as party to this Agreement may be terminated as outlined in Clauses 3.2 or 10.7.1 or under the following circumstances:

(i) Each Party may terminate its own status as party to this Agreement at any time for convenience effective immediately upon written notice to the other Parties.

(ii) The respective Party materially breaches its Service commitments under this Agreement, and the other Parties have voted to remove such Party, in accordance with the SRID Governance rules, because the contribution of the respective Party to the SRID is not essential or another Party is able to fill in the role of the withdrawing Party.

(iii) The respective Party is in default of this Agreement, due to gross negligence or willful misconduct, after the defaulting Party was notified to remedy the default, and such default was not remedied within a reasonable period of time; provided, however, that such Party shall only be terminated for this cause pursuant to a vote made by the other Parties in accordance with the SRID Governance rules.

9.3. Except for termination pursuant to Clause 3.2, in any other case of termination, a written notice will be served to or by the exiting Party, and the effective date of termination will be 15 calendar days in advance following delivery/receipt of that notice (unless a longer time period is stated in that notice).

9.4. 8In its capacity as supervisory body responsible for the effective operation of the SRID, FOCA will oversee on the termination of a Party's status as party to this Agreement pursuant to Clauses 9.2(ii) or (iii) or Clause 10.8.1.

10. MISCELLANEOUS

10.1. Notices. Any notice, request, consent, claim, demand, waiver, or other communications under this Agreement has legal effect only if addressed to a Party in accordance with Clause 5.5. Any notice under this Agreement which is not related to a technical aspect will be made in writing and will be deemed effectively given: (a) when received, if delivered by hand, with signed confirmation of receipt; (b) when received, if sent by a nationally recognized overnight courier, signature required; (c) when sent, if by facsimile with confirmation of transmission, if sent during the addressee's normal business hours, and on the next business day, if sent after the addressee's normal business hours; and (d) on the third day after the date mailed by certified or registered mail, return receipt requested, postage prepaid.

10.2. Interpretation. For purposes of this Agreement: (a) the words "include," "includes," and "including" are deemed to be followed by the words "without limitation"; (b) the word "or" is not exclusive; (c) the words "herein," "hereof," "hereby," "hereto," and "hereunder" refer to this Agreement as a whole; (d) words denoting the singular have a comparable meaning when used in the plural, and vice-versa; and (e) words denoting any gender include all genders. Unless the context otherwise requires, references in this Agreement: (x) to clauses, sections, exhibits, schedules, attachments, and appendices mean the clauses, sections of, and exhibits, schedules, attachments, and appendices attached to, this Agreement; (y) to an agreement, instrument, or other document means such agreement, instrument, or other document as amended, supplemented, and modified from time to time to the extent permitted by the provisions thereof; and (z) to a statute means such statute as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder. The Parties intend this Agreement to be construed without regard to any presumption or rule requiring construction or interpretation against the Party drafting an instrument or causing any instrument to be drafted. The exhibits, schedules, attachments, and appendices referred to herein are an integral part of this Agreement to the same extent as if they were set forth verbatim herein.

10.3. Headings. The headings in this Agreement are for reference only and do not affect the interpretation of this Agreement.

10.4. Entire Agreement. The Original Agreement is amended and replaced in its entirety with this Agreement as of the Effective Date. This Agreement (including all Annexes attached hereto and any documents incorporated by reference herein) constitutes the sole and entire agreement of the Parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. It is hereby understood this Agreement does not affect or supersede, and the Parties remain bound by, the MoC, the NDA, and any and all other documents incorporated by reference therein, as such may be amended from time to time.

10.5. Subcontractors. Each Party shall be permitted to utilize subcontractors in connection with its performance under this Agreement, provided that each Party shall remain responsible for the performance of its subcontractors.

10.6. Assignment. Subject to Clause 10.5, no Party shall assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance under this Agreement without the prior written consent of the Technical Board in accordance with the SRID Governance rules, which consent shall not be unreasonably withheld, conditioned, or delayed. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation, or reorganization involving either Party (regardless of whether such Party is a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations, or performance under this Agreement for which the prior written consent of the Technical Board is required. No assignment, delegation, or transfer will relieve either Party of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this clause 9.6 is void. This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns.

10.7. Change of Control. During the Term, if any Party experiences a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction), then that Party will give written notice to other Parties within 30 days after the change of control.

10.8. Force Majeure.

10.8.1. Force Majeure Event. In no event will any Party be liable or responsible, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, when and to the extent such failure or delay is caused by any circumstances beyond such Party’s reasonable control (a "Force Majeure Event"), including acts of God, pandemics, epidemics, flood, fire, earthquake or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Agreement, national or regional emergency, strikes, labor stoppages or slowdowns or other industrial disturbances, passage of Law or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota, or other restriction or prohibition or any complete or partial government shutdown, or national or regional shortage of adequate power or telecommunications or transportation. If a Party experiences a Force Majeure Event that impairs or inhibits its performance and that continues substantially uninterrupted for a period of 30 days or more, then that Party may be terminated as a party to this Agreement by the other Parties pursuant to a vote by such other Parties in accordance with the SRID Governance rules.

10.8.2. Affected Party Obligations. In the event of any failure or delay caused by a Force Majeure Event, the affected Party shall give prompt written notice to the Technical Board stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

10.9. No Third-Party Beneficiaries. This Agreement is for the sole benefit of the Parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other Person any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

10.10. Independent Contractors. In performing its Services, each Party will act solely as an independent contractor, and nothing herein will be construed to create the relationship of employer and employee, partnership, principal and agent, or joint venturers as between any of the Parties or their personnel. Except as expressly contemplated by this Agreement, no Party will have any right or authority, and will not attempt to enter into any contract, commitment or agreement, or incur any debt or liability of any nature in the name of or on behalf of any other Party.

10.11. Amendment or Modification; Waiver. No amendment to or modification of or rescission, termination, or discharge of this Agreement is effective unless it is in writing and signed by an authorized representative of each Party. No waiver by any Party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

10.12. Severability. If any term or provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

10.13. Governing Law; Submission to Jurisdiction. This Agreement is governed by and construed in accordance with the internal laws of Switzerland without giving effect to any choice or conflict of law provision or rule that would require or permit the application of the laws of any jurisdiction other than those of Switzerland. Any legal suit, action, or proceeding arising out of or related to this Agreement or the licenses granted hereunder will be instituted exclusively in the Swiss courts of law. Exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement shall be Bern and each Party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding. Service of process, summons, notice, or other document by mail to such Party's address set forth herein shall be effective service of process for any suit, action, or other proceeding brought in any such court.

10.14. Joinder. From time to time, new parties that are approved to be added to this Agreement pursuant to the SRID Governance Rules pursuant (each a “New Party”) may be added as parties to this Agreement and the Standard Contractual Clauses by: (a) executing a joinder in substantially the same form as the form attached as Annex G to this Agreement; and (b) delivering a copy of the executed joinder to a representative of each of the other Parties to this Agreement.

10.15. Counterparts. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email, or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this Agreement. For good measure, the Parties will in any way send the original signature page to FOCA.

[Signature page follows]

SIGNATURE PAGE

Name of Party	Role	Signatory’s Name	Capacity	Signature	Place/Date

TECHNICAL ANNEX A: F3411-19 Performance Requirements

All references in the annexes without a footnote are linked to ASTM F3411-19

1. Discovery and SynchronisationService (DSS)

The requirements in this section apply exclusively to implementers of a DSS

- Authentication: DSS0010
- Encryption: DSS0020 / DSS0120
- API: DSS0030 (Annex A4 F3411)
- Data Storage: DSS0040
- Data Requirement: DSS0130
- Use of Common Data Dictionary
- Manage Capacity & Fair Use
    - Subscription per area: DSS0050
    - Duration of subscription: DSS0060
- Region: DSS0110
- Implementation of instances: DSS0070
- Anything else on top of the standard?
- Persistent Test Interface: SP and DSS

The requirements in this section apply to Net-RID Service Providers or Net-RID Display Providers interacting with a DSS.

- Discoverability: NET0610
- Failure to create ISA: NET0620
- Query limitation (anti-scrapping): NET0630[51]
- Extrapolation
- Anything else on top of the standard?

2. U-space Service Providers (USSP)

The requirements in this section address interfaces between Net-RID Service Providers and Display Providers

2.1. NET-RID Service Provider

- Authentication and Encryption ()
- API: NET0340 / NET0710 (Annex A4 F3411)
- Maximum query area: NET0250
- Response time: NET0260
- Near real-time position: NET0270
- Support Non-Equipped Network Participants NET0110
- Loss of connectivity and extrapolation: NET0280 / NET0290 / NET0300 / NET0310 / NET 0320

2.2. NET-RID Display Provider

- API: NET0340 / NET0730 (Annex A4 F3411)
- Authentication: NET0210
- Data Retention: NET0330
- Obfuscation
- Encryption: NET0220
- Maximum query area: NET0240
- Query limitation (anti-scrapping): NET0230 / NET0720

TECHNICAL ANNEX B: Testing

1. DSS

DSS implementations are tested as part of a Net-RID Service Provider or Net-RID Display Provider, or both, when a new or modified DSS is being introduced.

The test requirements are defined in the F3411-19 standard, namely:

- DSS providers: persistent test environment (DSS0210),
- Anything on top of requirements set in DSS Compliance Matrix for DSS updates (TABLE A2.1):

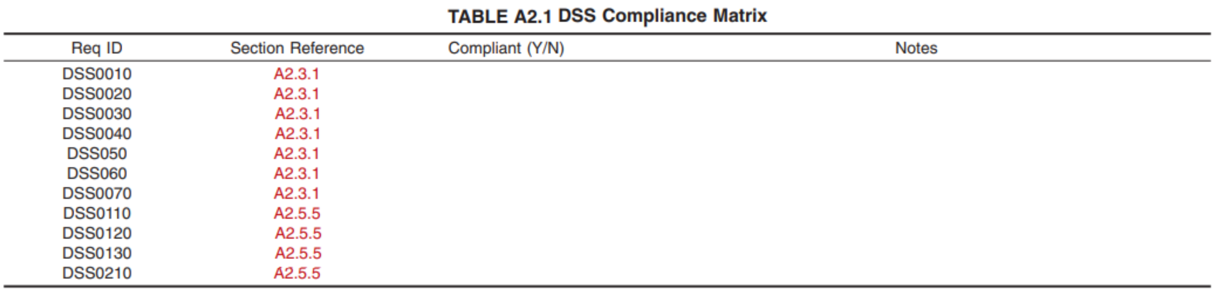

TABLE A2.1 DSS Compliance Matrix

Req ID	Section Reference	Compliant (Y/N)	Notes
DSS0010	A2.3.1		
DSS0020	A2.3.1		
DSS0030	A2.3.1		
DSS0040	A2.3.1		
DSS050	A2.3.1		
DSS060	A2.3.1		
DSS0070	A2.3.1		
DSS0110	A2.5.5		
DSS0120	A2.5.5		
DSS0130	A2.5.5		
DSS0210	A2.5.5		

2. USSP
   2.1. Testing

Participants shall be compliant with the Technical Annex A of the Master Agreement and shall have successfully completed the automated testing defined by the InterUSS project from the Linux Foundation or other equivalent process.

2.2. F3411-19 Testing Requirements

The test requirements are set in the Network Compliance Matrix (TABLE 23) of the F3411-19 Standard:

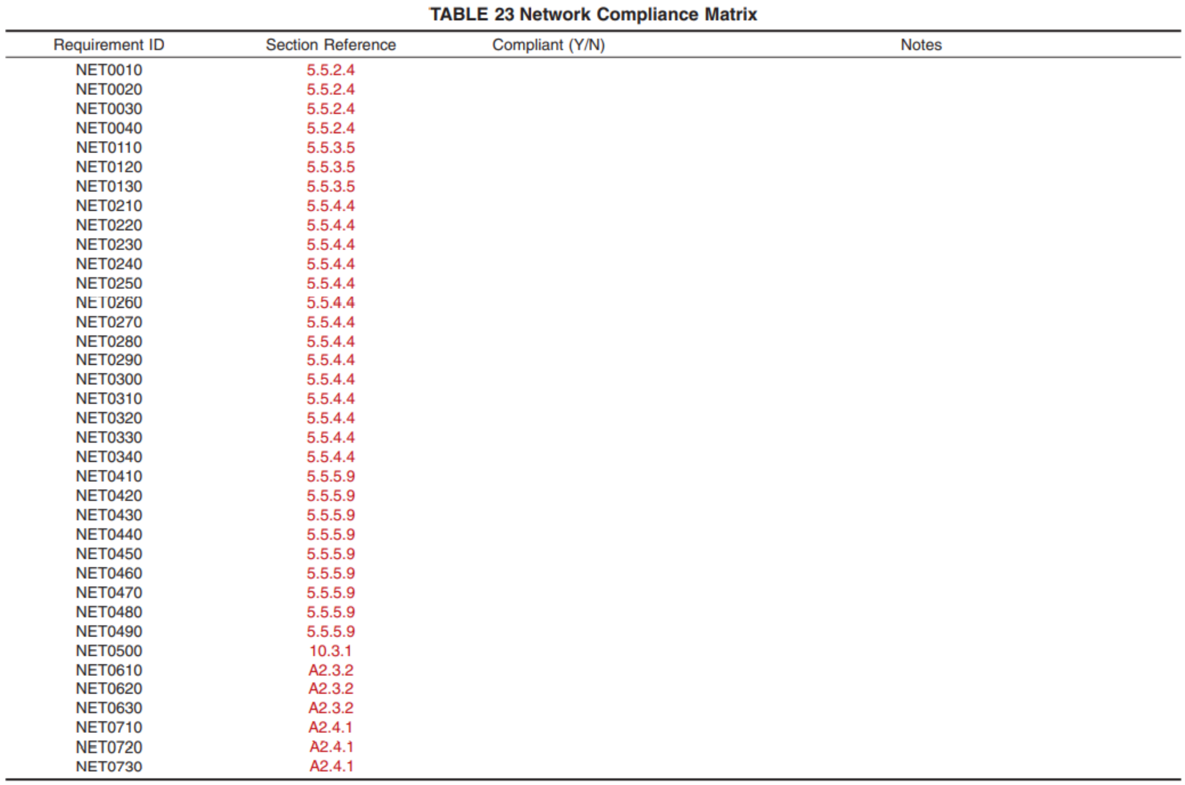

TABLE 23 Network Compliance Matrix

Requirement ID	Section Reference	Compliant (Y/N)	Notes
NET0010	5.5.2.4		
NET0020	5.5.2.4		
NET0030	5.5.2.4		
NET0040	5.5.2.4		
NET0110	5.5.3.5		
NET0120	5.5.3.5		
NET0130	5.5.3.5		
NET0210	5.5.4.4		
NET0220	5.5.4.4		
NET0230	5.5.4.4		
NET0240	5.5.4.4		
NET0250	5.5.4.4		
NET0260	5.5.4.4		
NET0270	5.5.4.4		
NET0280	5.5.4.4		
NET0290	5.5.4.4		
NET0300	5.5.4.4		
NET0310	5.5.4.4		
NET0320	5.5.4.4		
NET0330	5.5.4.4		
NET0340	5.5.4.4		
NET0410	5.5.5.9		
NET0420	5.5.5.9		
NET0430	5.5.5.9		
NET0440	5.5.5.9		
NET0450	5.5.5.9		
NET0460	5.5.5.9		
NET0470	5.5.5.9		
NET0480	5.5.5.9		
NET0490	5.5.5.9		
NET0500	10.3.1		
NET0610	A2.3.2		
NET0620	A2.3.2		
NET0630	A2.3.2		
NET0710	A2.4.1		
NET0720	A2.4.1		
NET0730	A2.4.1		

2.3. Automated testing

A certificate is issued by FOCA to all participants who successfully complete the automated testing. This certificate is valid until the next iteration of the automated testing.

FOCA notifies the participants of the next iteration of the automated testing 20 working days in advance.

TECHNICAL ANNEX C: SLA Lifecycle

1. Reporting: The Parties will provide quarterly reports to the Technical Board containing information on actual performance of Service achieved, compared to Service levels agreed on.

2. Reviews: The purpose of a review is to: review Service delivery since the last review, to discuss major deviations from Service provision, to negotiate potential changes to the SLA and to address concerns about Service provision. There will be 2 types of reviews:

   Ordinary: The Parties will hold annual reviews of this Agreement during at least 2 consecutive sessions, one to address all details and another to make a decision with respect to any changes to be made to this Agreement as a consequence of such ordinary review.

   Extraordinary: Whenever a Party deems necessary to review this Agreement, it shall so notify all signatory Parties (as such may change from time to time) and launch a process similar to the one for the ordinary review. Related sessions should start within a maximum 2 weeks as of such notification and will follow the above path.

   The Designated Review Owner (“Document Owner”) is responsible for facilitating regular reviews of this document. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

   Designated Review Owner: Amanda Boekholt

   Review Period: September 2021

   Previous Review Date: Octobre 2020

   Next Review Date: tbd

   This Agreement will be posted to the following location and will be made accessible to all stakeholders: Document Location: SUSI SharePoint and Mühlestrasse2, CH-3063 Ittigen.

3. Change Process

   This Agreement may be changed in accordance with the below:

   (i) Changes may not occur more often than quarterly, unless all Parties so agree or such change is due to change in regulations which is of immediate effect.

   (ii) In all cases, proposed changes must be reasonably motivated and accepted by the Parties, as per the SRID Governance rules.

   (iii) Without prejudice to the above, any Party may request a change of this Agreement to the rest of the Parties which shall decide in accordance with the rules herein.

   (iv) A change log will be added as an annex to this Agreement, to keep record of all such changes.

ANNEX D: SRID DATA SHARING AGREEMENT

This Data Sharing Agreement is an annex to the Master Agreement, as at the same date and under the same conditions indicated therein (the “Effective Date”)

BACKGROUND

(A) Any Party may be sharing Personal Information (the “Data Discloser”) with another Party (the “Data Receiver”) as part of the Services performed under the Master Agreement.

(B) The Parties agree to use the Personal Information on the terms set out in this Data Sharing Agreement.

(C) This is an annex to the Master Agreement.

AGREED TERMS

1. INTERPRETATION

The following definitions and rules of interpretation apply in this agreement. Notwithstanding, the terms capitalized and not otherwise defined herein shall have the meaning assigned to them in the Master Agreement.

1.1. Definitions:

“Agreed Purpose”: has the meaning given to it in clause 2 of this Data Sharing Agreement.

“Data Sharing Agreement”: this Data Sharing Agreement, which is an annex to the Master Agreement.

“Data Protection Legislation”: means all applicable laws, concerning Personal Information, primarily the Federal Act on Data Protection, SR. 235.1, but including, secondarily, to the extent applicable, the GDPR and any other similar legislation applicable concerning the Processing of Personal Information.

“Data Subject” means a person to whom Personal Information pertains to.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679).

“Master Agreement” means the agreement to which this Data Sharing Agreement is an annex to, whereby the Parties agreed on the main terms and conditions governing their relationship with respect to the SRID.

“Personal Information” means all information relating to an identified or identifiable person.

“Processing” means any operation with Personal Information, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data.

"Security Breach" means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed.

“Sensitive Personal Data” means Personal Information revealing: (i) religious, ideological, political or trade union-related views or activities, (ii) health, the intimate sphere or the racial origin, (iii) social security measures or (iv) administrative or criminal proceedings and sanctions.

“Shared Personal Information” means the Personal Information to be shared between the Parties under Section 4 of this Agreement.

“Subject Access Request” means the exercise by a Data Subject of his or her rights under the Data Protection Legislation.

“Term” means the duration of the Master Agreement and of this Agreement.

2. PURPOSE

2.1. This Data Sharing Agreement sets out the framework for the sharing of Personal Information when one Party discloses Personal Information to another in connection with the Master Agreement. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

2.2. The Parties consider this data sharing initiative necessary as to participate in the SRID. The aim of the data sharing initiative is to allow the sharing and display of UAS remote ID data, which may include Personal Information and operational data including but not limited to UAS ID, flight/operation description, pilot/operator ID, geolocation/telemetry information, including but not limited to latitude, longitude, geodetic altitude, pressure altitude, height, direction, operator latitude, operating area radius, operating area polygon, operator longitude, and authentication data, between the Parties, as necessary, to further display such data publicly.

2.3. The Parties agree to only Process Shared Personal Information, as described in clause 4.1, for the remote identification of drones.

The Parties shall not Process Shared Personal Information in a way that is incompatible with the purposes described in this section (Agreed Purpose).

3. COMPLIANCE WITH DATA PROTECTION LEGISLATION

Each Party must ensure compliance with applicable Data Protection Legislation at all times during the Term.

4. SHARED PERSONAL INFORMATION

The following types of Personal Information will be shared between the Parties during the Term of this agreement:

(a). Remote ID Data required by the ASTM standard: As defined in the Common Data Dictionary of the ASTM F3411-19 (Remote ID and Tracking) working group standard, including its successor standard, which may be updated from time to time, the required and optional data fields for Remote ID will be shared, including minimum characteristics that must be supported by both network and broadcast implementations. Such data fields include but are not limited to personal and operational information of a UAS flight such as UAS ID, flight/operation description, pilot/operator ID, geolocation/telemetry information, including but not limited to latitude, longitude, geodetic altitude, pressure altitude, height, direction, operator latitude, operating area radius, operating area polygon, operator longitude, and authentication data.

5. LAWFUL, FAIR AND TRANSPARENT PROCESSING

5.1. Each Party shall ensure that it Processes the Shared Personal Information fairly and lawfully in accordance with Section 5.2 during the Term of this Data Sharing Agreement.

5.2. Each Party shall ensure that it has legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal Information.

5.3. The Data Discloser shall, in respect of Shared Personal Information, ensure that it provides clear and sufficient information to the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will Process their Personal Information, the legal basis for such purposes and such other information as is required by Data Protection Legislation including:

(a). if Shared Personal Information will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer; and

(b). if Shared Personal Information will be transferred outside the European Economic Area ("EEA") pursuant to Clause 9.3 of this Data Sharing Agreement, that fact and sufficient information about such transfer, the purpose of such transfer and the safeguards put in place by the Data Receiver to enable the Data Subject to understand the purpose and risks of such transfer; and

(c). notice in its relevant privacy policy that Shared Personal Information will be shared with SUSI members (with reference to the following URL: https://susi.swiss/susi-members/) for uses permitted by this Agreement.

6. DATA QUALITY

6.1. Shared Personal Information must be limited to the Personal Information described in Clause 4.1 of this Data Sharing Agreement.

7. DATA SUBJECTS' RIGHTS

7.1 The Parties each agree to provide such assistance as is reasonably required to enable the other Party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.

7.2 Each Party is responsible for maintaining a record of individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

8. DATA RETENTION AND DELETION

8.1. A Data Receiver shall not retain or Process Shared Personal Information for longer than is necessary to carry out the Agreed Purpose. For the avoidance of any doubt, unless expressly required by Data Protection Legislation, a Display Provider will not retain such information for longer than stated in the Standard.

8.2. Notwithstanding clause 8.1, Parties shall continue to retain Shared Personal Information in accordance with any statutory or professional retention periods applicable in their respective countries and / or industry, to the maximum extent permitted by the Swiss law and the Data Protection Legislation.

8.3. The Data Receiver shall ensure that any Shared Personal Information are returned to the Data Discloser or destroyed in the following circumstances, whichever occurs earlier:

(a) on termination of the Data Sharing Agreement;

(b) on expiry of the Term; or

(c) once Processing of the Shared Personal Information is no longer necessary for the purposes it was originally shared for, as set out in Clause 2.3.

8.4. Upon request, following the deletion of Shared Personal Information in accordance with Clause 8.3, the Data Receiver shall notify the Data Discloser that the Shared Personal Information in question has been deleted.

9. TRANSFERS

9.1. For the purposes of this clause, transfers of Shared Personal Information shall mean any sharing of Shared Personal Information by the Data Receiver with a third party, and shall include, but is not limited to, the following:

(a) subcontracting the Processing of Shared Personal Information;

(b) granting a third-party controller access to the Shared Personal Information.

9.2. If the Data Receiver appoints a third-party processor to Process the Shared Personal Information it shall remain liable to the Data Discloser for the acts or omissions of such third-party processor.

9.3. The Parties will enter into controller-to-controller standard contractual clauses (attached as Annex G) as adopted by the European Commission and recognized by the Federal Data Protection and Information Commissioner to enable the transfer of Shared Personal Information of Swiss residents to any Party located in a country not approved by the supervisory authority in Switzerland as providing adequate protection. The Data Receiver may not further transfer Shared Personal Information of Swiss residents to a third party located outside Switzerland unless it:

(a) complies with the provisions of Articles 26 of the GDPR, as applicable (in the event the third party is a joint controller); and

(b) ensures that (i) the transfer is to a country approved by the supervisory authority in Switzerland as providing adequate protection pursuant to Article 7 of the Ordinance on the Federal Act on Data Protection; (ii) there are appropriate safeguards in place pursuant to Art. 6 Federal Act on Data Protection (FADP); or (iii) one of the derogations for specific situations under the FADP applies to the transfer.

10. SECURITY AND TRAINING

10.1 With respect to any Shared Personal Information in a Party's possession or control, such Party undertakes to have in place throughout the Term appropriate technical and organizational security measures designed to:

(a) prevent:

(i) the unauthorized or unlawful Processing of the Shared Personal Information; and

(ii) the accidental loss or destruction of, or damage to, the Shared Personal Information

(b) ensure a level of security appropriate to:

(i) the harm that might result from such unauthorized or unlawful Processing or accidental loss, destruction or damage; and

(ii) the nature of the Shared Personal Information to be protected.

10.2 The Parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the Term.

10.3 It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and Process the Shared Personal Information in accordance with the technical and organizational security measures together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the Processing of personal information.

10.4 The level, content and regularity of training referred to in Clause 10.3 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and Processing of the Shared Personal Information.

11. SECURITY BREACHES AND REPORTING PROCEDURES

11.1 Each Party shall comply with its obligation to report a Security Breach to the appropriate government authority and (where applicable) Data Subjects under the applicable Data Protection Legislation and shall each inform the other Parties of any Security Breach irrespective of whether there is a requirement to notify any government authority or Data Subject(s).

11.2 The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Security Breach in an expeditious and compliant manner.

12. REVIEW AND TERMINATION OF AGREEMENT

12.1. Parties shall review the effectiveness of this data sharing initiative as part of the review of the entire Master Agreement, as per the provisions thereof, having consideration to the aims and purposes set out in Clauses 2.2 and 2.3.

12.2. The review of the effectiveness of the data sharing initiative will involve:

(a) assessing whether the purposes for which the Shared Personal Information is being Processed are still the ones listed in Clause 2.3. of this Data Sharing Agreement;

(b) assessing whether the Shared Personal Information is still as listed in Clause 4.1 of this Data Sharing Agreement;

(c) assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and

(d) assessing whether Security Breaches involving the Shared Personal Information have been handled in accordance with this Data Sharing Agreement and the applicable legal framework.

12.3. Each Data Discloser reserves its rights to inspect a Data Receiver 's arrangements for the Processing of Shared Personal Information (pursuant to any frequency, scope, conditions and parameters reasonably required by such Data Receiver).

12.4. This Data Sharing Agreement may be terminated in accordance with the relevant conditions in the Master Agreement and in any case at the same time as the Master Agreement.

13. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR GOVERNMENT AUTHORITIES

13.1. In the event of a dispute or claim brought by a Data Subject or the competent government authority concerning the Processing of Shared Personal Information against a Party, that Party will inform the other Parties about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

13.2. The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the competent government authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

13.3. Each Party shall abide by a decision of a competent court or of the competent government authority.

14. WARRANTIES

14.1. Each Party warrants and undertakes that it will:

(a) Process the Shared Personal Information in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its Shared Personal Information Processing operations.

(b) Promptly respond and as far as reasonably possible to enquiries from the relevant government authority in relation to the Shared Personal Information.

(c) Respond to Subject Access Requests in accordance with the Data Protection Legislation.

(d) Where applicable, maintain registration with all relevant supervisory authorities to Process all Shared Personal Information for the Agreed Purpose.

(e) Take all appropriate steps designed to ensure compliance with the security measures set out in Clause 10 above.

14.2. The Data Discloser warrants and undertakes that it is entitled to provide the Shared Personal Information to the Data Receiver.

14.3. The Data Recipient warrants and undertakes that it will not disclose or transfer Shared Personal Information outside the EEA unless it complies with the obligations set out in Clause 9.3 above.

14.4. Except as expressly stated in this Data Sharing Agreement or in the Master Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

15. INDEMNITY

15.1. Each Party undertakes to indemnify the other Parties and hold the other Parties harmless from any cost, charge, damages, expense or loss which it causes the other Parties to the extent arising from its breach of any of the provisions of this Data Sharing Agreement, except to the extent that any such liability is excluded under, and only to the extent of the liability limits provided under, Clause 17.1.

15.2. Indemnification hereunder is contingent upon:

(a) the Party to be indemnified (the indemnified Party) promptly notifying the other Party (the indemnifying Party) of a claim,

(b) the indemnifying Party having sole control of the defense and settlement of any such claim, and

(c) the indemnified Party providing reasonable co-operation and assistance.

16. ALLOCATION OF COST

Each Party shall perform its obligations under this Data Sharing Agreement at its own cost.

17. LIMITATION OF LIABILITY

17.1. TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) LOSS OF PRODUCTION, USE, BUSINESS, REVENUE, OR PROFIT OR DIMINUTION IN VALUE; (b) LOSS OF GOODWILL OR REPUTATION; OR (c) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES, REGARDLESS OF WHETHER SUCH PERSONS WERE ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE, AND NOTWITHSTANDING THE FAILURE OF ANY AGREED OR OTHER REMEDY OF ITS ESSENTIAL PURPOSE. THE AGGREGATE LIABILITY OF EACH PARTY TO ALL OTHER PARTIES ARISING FROM OR RELATED TO THIS AGREEMENT WILL NOT EXCEED 100,000 SWISS FRANCS.

18. FURTHER ASSURANCES

On a Party's reasonable request, the other Party shall, at the requesting Party's sole cost and expense, execute and deliver all such documents and instruments, and take all such further actions, as may be necessary to give full effect to this Data Sharing Agreement.

19. RELATIONSHIP OF THE PARTIES

The relationship between the Parties is that of independent contractors. Nothing contained in this Data Sharing Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the Parties, and neither Party shall have authority to contract for or bind the other Party in any manner whatsoever.

20. CHANGES TO THE APPLICABLE LAW

If during the Term the Data Protection Legislation change in a way that the Data Sharing Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree to negotiate in good faith to review the Data Sharing Agreement in the light of the new legislation.

TECHNICAL ANNEX E: POINTS OF CONTACT

Organization	Overall contact	Technical contact
	name, role/job title, address, telephone, and email	name, role/job title, address, telephone, and email

ANNEX F: END USER TERMS

References to “you” below shall refer to End Users. Each Party should adjust bracketed words to reflect appropriate terms used in its Terms of Service. If any term below is not permitted by the law of your jurisdiction, it may be adjusted only to the minimum extent necessary to accommodate such legal requirements.

1. You may only use the [End User Services] for non-commercial testing and evaluation purposes that are authorized by [us].

2. You must comply with all applicable laws when using the [End User Services]. Do not use the [End User Services], including any information provided by or through the [End User Services], in a way that is inappropriate, illegal, or in violation of others' rights (including privacy, publicity, and intellectual property rights).

3. The [End User Services] are not designed to identify all unmanned aerial systems (“UAS”) that are operating. Even if the [End User Services] do not indicate any UAS in a selected area, [we] do not guarantee that there are no UAS in that area and we do not recommend or endorse the safety or legality of your use of UAS in that area. You are solely responsible for your use of the [End User Services].

4. The [End User Services] do not provide and may not be used to determine flight restrictions or rules. At all times, UAS operators must check official sources to determine whether it is safe or legal to operate a UAS for their desired flight.

5. The [End User Services] may not be available at all times and should only be used for general informational purposes. The [End User Services] are not designed for mission-critical operations or any uses that require 24/7 availability or fail-safe operation.

6. Certain information displayed through or provided as part of the End User Services is made available by or on behalf of third parties (each, a “Third-Party Supplier”). Notwithstanding anything in [these Terms] to the contrary, to the fullest extent permitted by applicable law, [we] and [our][] Third-Party Suppliers will not be liable to you under any theory of liability, whether based in contract, tort, negligence, warranty, or otherwise, for any direct, indirect, consequential, incidental, or special damages or lost profits, even if [we] or [our] Third-Party Suppliers have been advised of the possibility of such damages. [Our] Third-Party Suppliers will be considered third-party beneficiaries for purposes of enforcing this Section [6].

ANNEX G: FORM OF JOINDER

This Joinder (this "**Joinder**") to the Amended and Restated Swiss Remote Identification Master Agreement, with an effective date of [Insert] (as further amended or modified, the "**Agreement**") is made and entered into as of the date that the new party identified in the signature block below ("**New Party**") signs this Joinder. Capitalized terms used but not otherwise defined herein shall have the meanings set forth in the Agreement.

Background

Pursuant to Section 9.17 of the Agreement, the New Party desires to become a party to the Agreement and each of the Standard Contractual Clauses by executing this Joinder.

NOW, THEREFORE, IN CONSIDERATION of the promises provided herein and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the New Party agrees as follows:

Agreement

The New Party acknowledges and agrees that it: (a) has received and reviewed a complete copy of the Agreement, including the Standard Contractual Clauses attached thereto; (b) shall become a party to the Agreement and the Standard Contractual Clauses upon execution of this Joinder and thereafter be deemed a "Party" under the Agreement; (c) shall be fully bound by, and subject to, all of the covenants, terms and conditions of the Agreement (including the attached Standard Contractual Clauses), and entitled to all the benefits thereof, as though an original party thereto; and (d) shall deliver an executed copy of this Joinder to a representative of each of the Parties to the Agreement.

Signed by the New Party's authorized representative on the date indicated below.

New Party:

[Insert Name]

Name:________________

Position:______________

Signature:____________________

Date:_________________

ANNEX H: Standard Contractual Clauses

SECTION I

(II) *CLAUSE 1*

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(III) *CLAUSE 2*

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

(IV) *CLAUSE 3*

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.5 (e) and Clause 8.9(b);

(iii) The Parties have omitted this exception from these standard contractual clauses because it does not apply to controller-to-controller data transfers;

(iv) Clause 12 - Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

(V) *CLAUSE 4*

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

(VI) *CLAUSE 5*

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

(VII) *CLAUSE 6*

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

(VIII) *CLAUSE 7*

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

(IX) *CLAUSE 8*

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 **Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 **Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

(X) *CLAUSE 9*

Use of sub-processors

The Parties have omitted this clause from these standard contractual clauses because it does not apply to controller-to-controller data transfers.

(XI) *CLAUSE 10*

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

(XII) *CLAUSE 11*

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them..

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

(XIII) *CLAUSE 12*

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

(XIV) *CLAUSE 13*

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

(XV) *CLAUSE 14*

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

(XVI) *CLAUSE 15*

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

(XVII) *CLAUSE 16*

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

(XVIII) *CLAUSE 17*

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.

(XIX) *CLAUSE 18*

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Switzerland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I to Standard Contractual Clauses

A. **LIST OF PARTIES**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. **Name**: ……………………………………………………………………………………………………

Address: ……………………………………………………………………………………………………

Contact person's name, position and contact details: ………………………………………………
Activities relevant to the data transferred under these Clauses: As described in the "role" column on the signature page to the Agreement.
Signature and date: …………………………………………………………………………………………

Role (controller/processor): Controller

2. ……

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. **Name**: ……………………………………………………………………………………………………

Address: ……………………………………………………………………………………………………

Contact person's name, position and contact details: ………………………………………………
Activities relevant to the data transferred under these Clauses: As described in the "role" column on the signature page to the Agreement.
Signature and date: …………………………………………………………………………………………

Role (controller/processor): Controller
2. ……

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Operators of UAS.

Categories of personal data transferred

Remote ID Data required by the ASTM standard: As defined in the Common Data Dictionary of the ASTM F3411-19 (Remote ID and Tracking) working group standard, including its successor standard, which may be updated from time to time, the required and optional data fields for Remote ID will be shared, including minimum characteristics that must be supported by both network and broadcast implementations. Such data fields include but are not limited to personal and operational information of a UAS flight such as UAS ID, flight/operation description, pilot/operator ID, geolocation/telemetry information, including but not limited to latitude, longitude, geodetic altitude, pressure altitude, height, direction, operator latitude, operating area radius, operating area polygon, operator longitude, and authentication data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

As described in the Agreement.

Purpose(s) of the data transfer and further processing

To facilitate participation in the national implementation of remote identification for UAS in Switzerland, as further described in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data will be retained only as necessary to carry out the purposes of processing, for no longer than as permitted under the Standard 3411-19 issued by ASTM, or as required under applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter and nature of transfers to processors is set forth in the applicable processor agreement between each party and its processor. The duration of the transfer to each processor is for the term of the applicable processor agreement.

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

The Federal Data Protection and Information Commissioner.

ANNEX II to Standard Contractual Clauses

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Access Controls. Each Party will implement reasonable measures designed to comply with the following access control objectives: (a) abide by the "principle of least privilege," pursuant to which the Party will permit access to Shared Personal Information by its personnel solely on a need-to-know basis; (b) promptly terminate its personnel's access to Shared Personal Information when such access is no longer required for performance under the Agreement; and (c) be responsible for any processing of Shared Personal Information by its personnel.

2. Account Management. Each Party will implement reasonable measures designed to manage the creation, use, and deletion of all account credentials used to access the Shared Personal Information.

3. Vulnerability Management. Each Party will implement reasonable vulnerability management measures designed to monitor for unauthorized access to Shared Personal Information through logging and event monitoring. Each Party will implement software updates and patches made available by applicable third-party software providers following release.

4. Security Segmentation. Each Party will implement reasonable measures designed to monitor, detect and restrict the flow of information on a multi-layered basis within its network systems using tools such as isolation layers, proxies, sandboxes, and network-based intrusion detection systems.

5. Encryption. Each Party will implement reasonable measures designed to encrypt, using industry standard encryption tools, Shared Personal Information that it: (a) transmits or sends wirelessly or across public networks; (b) stores on laptops or storage media, (c) stores on portable devices or, at least at the container level, at rest within such party's computing environment, and (d) is required by applicable law to encrypt. Each Party will implement reasonable measures designed to safeguard the security and confidentiality of all encryption keys associated with encrypted information.

6. Physical Safeguards. Each Party will implement reasonable physical access controls designed to protect relevant computing equipment owned or controlled by such Party for the purpose of processing Shared Personal Information, including an access control system designed to enable such Party to control physical access to each facility it owns or controls.

7. Administrative Safeguards. Prior to providing access to Shared Personal Information to any of its personnel, each Party will implement reasonable measures designed to evaluate the reliability of such personnel. Each Party will require its personnel to sign reasonable confidentiality agreements that apply to their processing of Shared Personal Information.

SWISS ADDENDUM TO STANDARD CONTRACTUAL CLAUSES

The Clauses will be interpreted in accordance with the following:

1. References to the General Data Protection Regulation refer instead to the Federal Act on Data Protection of 19 June 1992 (the "**FADP**"), and after its entry into force, will refer to the revised version of the FADP.

2. References in the Clauses to a "Member State" and "EU Member State" will not be read to prevent Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland), and until the revised FADP enters into force, the Standard Contractual Clauses will also protect the data of legal entities in Switzerland.