9.4 The Partial contract shall be valid upon signature by the Customer and the Contractor and shall enter into force on the day when it is registered in the Register of Contracts according to Act. No. 340/2015 Coll., on the Register of Contracts, as amended.

9.5 **The Partial contract has been signed electronically, only in one electronic copy**.

9.6 The following Annexes shall form an inseparable part of this Partial contract: *****

***** *The Contracting Parties shall add the list of relevant Annexes and shall add them to the Partial contract.*

Annex 1 – System development specification

Annex 2 – Price calculation

Annex 3 – Delivery dates and Milestones

……..
Air Navigation Services of the Czech Republic (ANS CR)
Customer
Jan Klas
Director General

……
FREQUENTIS California Inc.
Contractor

XXX
xxx

Annex 2 – Cyber Security

Contractual ensuring of measures in the area of information and cybersecurity within the meaning of Section 8 (2) of the Regulation No. 82/2018 on security measures, cybersecurity incidents, reactive measures, requirements for filing in the area of cybersecurity, and data removal (the Cybersecurity Regulation), as amended

1. Preamble

1.1 The Contractor understands and acknowledges that it is a major contractor according to Section 2 (n) of the Cybersecurity Regulation for the Customer, which is Air Navigation Services of the Czech Republic (ANS CR), who is an administrator of information and communication systems of the critical information infrastructure.

1.2 The following are the information/communication systems the role of a major contractor relates to: **NOTAM/OPMET including sub-system IBS, AMHS/AFTN**.

1.3 The Contractor undertakes to comply with the requirements of the information security management system specified in this Annex and in the Security rules distributed in compliance with Article 4 hereof.

2. Definitions of Terms

2.1 “Asset” shall mean a summary of information and services that are necessary for the operation of the information/communication system referred to in Article 1.2 hereof.

2.2 “Security Incident” shall mean violation of the information security in the information/communication system referred to in Article 1.2 hereof.

2.3 “Security Measure” shall mean an act the aim of which is to ensure information security in the information/communication system referred to in Article 1.2 hereof, its availability and reliability in the cybernetic space.

2.4 “Security Policy” shall mean a set of rules and principles determining the manner of ensuring of the assets protection.

2.5 “Security Event” shall mean an event that may violate the information security in the information/communication system referred to in Article 1.2 hereof.

2.6 “Contractor” shall mean a Contractor according to the Agreement who is also a major contractor according to Section 2 (n) of the Cybersecurity Regulation.

2.7 “Critical Information Infrastructure” shall mean an element or a system of elements that are necessary for the operation of the information/communication system referred to in Article 1.2 hereof.

3. Information Security

3.1 The Contractor is obliged to implement and realize security measures according to this Annex as required for ensuring of security of the information/communication systems referred to in Article 1.2 hereof and maintain appropriate security documentation.

3.2 The Security Measures set out in in this Annex shall be set in line with the requirements of the Act No. 181/2014 Coll., on cybernetic security and on amendments to related acts (the

Cybersecurity Act), as amended, the requirements of the Cybersecurity Regulation and the CSN ISO/IEC 27001 standard.

3.3 The Customer shall verify the implementation and realisation of the Security Measures in compliance with Article 8 hereof or through a valid certificate of ISO/IEC 27001, or through a different established, valid and internationally recognized information security management system at the Contractor.

4. Adherence to Customer's Security Policies

4.1 The Contractor shall comply with the "Security Rules for Major Contractors" of the Customer that are available at the following websites:

https://www.ans.cz/content/documents/Security_rules_for_major_contractors.pdf

(hereinafter referred to as the "**Security Rules**"). The Contractor hereby confirms that he got to know the Security Rules and agrees with them.

4.2 The Customer is obliged, via the cyber security manager, to provide the Contractor with Security Rules supplemented with details of Customers security standards within 10 days from the effectiveness of the Agreement. Such supplemented Security Rules shall be distributed by electronically signed e-mails.

4.3 The Customer may, in connection with legislative changes, decisions or warnings from the National Cyber and Information Security Agency, decisions of other administrative authorities and/or fulfilment of remedial measures resulting from state supervision, after Agreement signature change the Security Rules from time to time. The amended Security Rules shall be distributed in electronic (digital) form, meaning email with attachments converted in pdf format and signed by Cyber Security manager with recognized electronic signature (in accordance with eIDAS), databox or in the form of letter signed by Cyber Security manager sent via the holder of postal licence with confirmation of delivery on the address of Contractor`s Cyber Security Manager. In case the Contractor does not disagree with the amended Security Rules within 10 working days from the delivery of its announcement, it is considered to agree with amendment and the Contractor shall comply with such amended Security Rules.

4.4 The Contractor shall make sure that all its employees who participate in performance of the obligations as defined herein or in the Agreement have been provably acquainted with the Security Rules.

5. Change Management

5.1 The Contractor is required to manage risk associated with the performance of the Agreement including residual risk. If requested by the Customer's Cybersecurity manager or by persons conducting the control activity as defined in Article 8 hereof, the Contractor is required to document the risk management method.

5.2 The Contractor understands and acknowledges that the Customer implements changes in compliance with Section 11 of the Cybersecurity Regulation.

5.3 As regards major changes, the Customer carries out a risk analysis in compliance with the CRAMM methodology, applying the RAMSES tool.

5.4 The Contractor shall provide the Customer with necessary cooperation and shall be helpful during change management, especially during regular risk assessment and every inspection of the Security Measures implemented and realized by persons appointed by the Customer. The Contractor shall ensure such cooperation also with his subcontractors.

5.5 If, within its solution required for provision of the services under the Agreement, the Contractor makes use of technical or programme tools of Huawei Technologies Co., Ltd.

or ZTE Corporation including their subsidiaries, the Contractor within the tender process submitted to the Customer a risk analysis prepared in compliance with the methodology of the National Cyber and Information Security Agency (NÚKIB).

6. **Notification Requirements**

6.1 The Contractor shall inform the Customer without undue delay via the Cybersecurity manager, if it identifies any breach of the information security caused by a cyber incident and shall provide the Customer with sufficient information allowing to meet all requirements, respond to the incident, investigate it and report it to the National Cyber and Information Security Agency in compliance with the requirements of the Cybersecurity Regulation. The Contractor is obliged to participate in such an effort and take financially reasonable steps requested by the Customer.

6.2 The Contractor shall use Customer´s Cybersecurity manager contact and inform the Customer on a continuous basis and without undue delay of all the threats and weaknesses the Contractor is aware of that might impact the risk assessment carried out by the Customer.

6.3 The Contractor shall inform the Customer´s Cybersecurity Manager without undue delay of a major change in the Contractor's control structure pursuant to the Business Corporations Act or of a change in the ownership of principal assets or of a change in the authorization to handle those assets used by the Contractor for the performance of the Agreement whereas a significant change in control means a change in the controlling entity pursuant to Section 74 et seq. of Act No. 90/2012 Coll., on Business Companies and Cooperatives (Business Corporations Act), as amended.

6.4 More detailed conditions of reporting and classification of security incidents are specified in the Security rules.

7. **Subcontractors**

7.1 In accordance with Section 105 (4) in conjunction with Section 3 of Act No. 134/2016 Coll., On Public Procurement, as amended, according to Czech law, the Contractor shall inform in writing in advance of its intention to use a subcontractor that the Contractor has not notified during the procurement procedure, including its identification and details of the activities to be carried out by the subcontractor and the data made available. Identification of the subcontractors who will be involved in the performance of the public contract after the conclusion of the contract, the subject of activities to be performed by the subcontractor and the data made available shall be communicated by the Contractor to the Customer prior to commencement of performance by the subcontractor concerned.

7.2 If the Contractor negotiates with a subcontractor to carry out activities or disclose data within the meaning of this Annex to the Agreement, the Contractor shall enter into a contract or other legal act with the subcontractor giving rise to the same rights and obligations in relation to information and cyber security as set out in this Annex. In particular, it is necessary to provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of the Regulation on Cyber Security.

7.3 In relation to each subcontractor, the Contractor shall:

a) make reasonable effort to check that the subcontractor provides the level of protection in the area of the information and cybersecurity as required by the Agreement;

b) make sure that in case of a chain of subcontractors their mutual rights and obligations as regards the information and cybernetic security are regulated through a written contract including terms and conditions offering at least the same level of protection as those that

are defined in the Agreement and are meeting the requirements of the applicable legislation relating to contractual performance;

c) provide the Customer at its request with copies of selected parts of contracts with subcontractors (or similar documents) relevant for performance of the Agreement;

d) make sure that every subcontractor meets the obligations arising out of the Agreement that apply to protection in the area of the information and cybersecurity executed by the subcontractor as if the subcontractor was a party to this Agreement instead of the Contractor.

7.4 In case that the Security Rules form an integral part of an agreement with subcontractors or between subcontractors, the Contractor shall inform the Customer in advance. The Customer is entitled to object within five working days of the notification of the need to provide Security Rules to subcontractors that the provision of Security Rules to subcontractors is not necessary or that the provision of Security Rules to a specific subcontractor entails a security risk. In this case, the Contractor must prove the necessary need to provide these Security Rules to a particular subcontractor or propose the use of another subcontractor. If the Customer finds this need justified or fails to assess the new subcontractor as a security risk, the Customer will allow to provide this safety information to the specific subcontractor.

8. Inspections and quality control

8.1 If requested, the Contractor and all subcontractors shall provide access to all information required for proving of compliance herewith and cooperate during audits and inspections conducted by any auditor authorized by the Customer. The Contractor shall ensure such cooperation also on the part of the subcontractor, if applicable.

8.2 The Customer shall inform the Contractor of such an inspection well ahead of time prior to the inspection. In addition, the Customer shall make reasonable effort to make sure that the inspection will not cause damage or disturb the premises, equipment, staff and activities of the Contractor in an excessive manner. The Contractor is not required to provide access to its premises during an inspection in the following situations:

a) The person conducting the inspection fails to present an identity card and an authorization to conduct the inspection;

b) The inspection is not conducted in the common working hours unless the inspection needs to be conducted beyond the common working hours and the inspector informed the Contractor of that fact in advance (during common working hours).

8.3 The Contractor understands and acknowledges that the Customer performs regular contractor assessment in compliance with the requirements of CSN EN ISO 9001 standard.

Annex No. 3 to the Agreement No. ANS CR 224/2022/IS/073 (hereinafter referred to as the "Agreement")

"Ensuring Protection of Personal Data pursuant to the Regulation of the European Parliament and Council (EU) 2016/679 of 27th April 2016 on protection of natural persons in association with the personal data processing and on free movement of such data and on cancellation of the Directive 95/46/ES (General Data Protection Regulation); (hereinafter referred to as the **"GDPR**)"

1. Definition of Terms

1.1 "**Personal Data**" shall mean for the purposes of this Annex and within the meaning of the GDPR, any and all information on an identified or identifiable natural person (hereinafter the "**Data Subject**"); an identifiable natural person shall mean a natural person who may be directly or indirectly identified, in particular with reference to a certain identified, such as name, identification number,location data, network identifier or to one or more special elements of physical, physiological, genetic, mental, economic, cultural and/or social identity of such a natural person.

1.2 **"Processing"** shall mean for the purposes of this Annex and within the meaning of the GDPR any operation or a set of operations with personal data or sets of personal data which is made with the use of automated procedures or without the use of automated procedures, such as collecting, recording, organizing, structuring, storage, adaptation or alteration, retrieving, consulting, use, disclosure by transmitting, dissemination and/or any other disclosure, alignment or combination, restriction, deletion or destruction.

1.3 **"Controller"** shall mean for the purposes of this Annex and within the meaning of the GDPR the natural person or legal entity, public authority, agency or another entity which by himself/herself/itself or together with others determines the purposes and means of personal data processing ; if such purposes and means of such processing are determined by the law of the Union or of a member state, such law may determine the Controller in question or the special criteria for determination of such a Controller. Controller within the sense of this Annex to the Agreement is **ANS CR**.

1.4 **"Processor"** shall mean for the purposes of this Annex and within the meaning of the GDPR the natural person or legal entity, public authority, agency or another entity processing the personal data on behalf of the Controller. Processor within the sense of this Annex to the Agreement is **Frequentis California, Inc.**, 2511 Garden Road, Suite A-165, Monterey 93940 California, UNITED STATES.

1.5 **"Sub-Processor"** shall mean for the purposes of this Annex and within the meaning of the GDPR the natural person or legal entity, public authority, agency or another entity (with the exception of the Processor's employee) who processes the personal data on the basis of an authorization from the Processor on behalf of the Controller. Sub-processor within the sense of this Annex to the Contract are

a) Frequentis Czech Republic s.r.o., with its registered office at Vyskočilova 1461/2a, Michle, 140 00 Praha 4, Czech Republic, Company Identification Number: 290 53 285, registered in the Commercial Register maintained by the Municipal Court in Prague, Section C, Insert 163146.

b) Neoware s.r.o., with its registered office at Vyskočilova 1461/2a, Michle, 140 00 Praha 4, Czech Republic, Company Identification Number: 24681288, registered in the Commercial Register maintained by the Municipal Court in Prague, Section C, Insert 165657.

1.6 "**Personal Data Security Breach**" shall mean for the purposes of this Annex and within the meaning of the GDPR a security breach which leads to accidental or unlawful destruction, loss,

change or unauthorized provision or disclosure of the transferred, stored or otherwise processed personal data.

2. Subject of Processing

2.1 The subject of personal data processing is in/for NOTAM/OPMET/IBS/AMHS/AFTN: access to NOTAM/OPMET/IBS/AMHS/AFTN administrators/operators and end-user's personal data during provision of service support.

3. Duration of Processing

3.1 The personal data will be processed for the period of: validity of the Agreement + 3 months.

4. Nature and Purpose of Processing

4.1 Nature and purpose of personal data processing are defined as follows: administration, configuration and management of NOTAM/OPMET/IBS/AMHS/AFTN system maintained and operated by ANS CR.

5. Type of Personal Data Processed

5.1 The personal data processed in/for NOTAM/OPMET/AMHS/AFTN are of the following type: login.

5.2 The personal data processed in/for IBS are of the following type: name and surname, mobile phone number, e-mail.

6. Categories of the Subject of the Personal Data Processed

6.1 The categories of the subject of the personal data processed in/for NOTAM/OPMET/IBS/AMHS/AFTN are the following: ANS CR employees.

7. Processor's Obligations

7.1 The Processor has to observe all the applicable legal regulations governing data protection, in particular the GDPR.

7.2 The Processor must not process the personal data provided by the Controller in any other way and for any other purpose than in conformity with the documented instructions by the Controller, unless the processing is required by the legal regulations in force which apply to such Processor. In this event, the Processor shall notify the Controller of such a legal requirement even before the processing of such personal data.

7.3 The Processor shall immediately notify the Controller in the event if, in the Processor's opinion, a certain instruction breaches the GDPR or other regulations of the European Union or of any member state related to personal data protection.

7.4 The Processor has to ensure that the persons authorized to process personal data are committed to confidentiality, unless the statutory obligation of confidentiality already applies to them.

7.5 Taking into account the state of the art, the implementation costs, nature, extent, context and purposes of processing as well as the different levels of probability and differently serious risks to rights and freedoms of Data Subjects, the Controller and the Processor shall make suitable technical and organizational measures to ensure the level of security corresponding to the particular risk, including the measures indicated in Art. 32 of the GDPR.

8. Sub-Processors

8.1 In accordance with Section 105 (4) in conjunction with Section 3 of Act No. 134/2016 Coll., On Public Procurement, as amended, the Processor shall inform in writing in advance of its intention to use a Sub-Processor that the Processor has not notified during the procurement procedure, including its identification and details of the activities to be carried out by the subcontractor and the personal data processed. Identification of the Sub-Processors who will be involved in the performance of the public contract after the conclusion of the contract, the subject of activities to be performed by the Sub-Processor and the personal data processed shall be communicated by the Processor to the Controller prior to commencement of performance by the Sub-Processor concerned.

8.2 If the Processor negotiates with a Sub-Processor to carry out activities or process personal data within the meaning of this Annex to the Agreement, the Processor shall enter into a contract or other legal act with the Sub-Processor giving rise to the same rights and obligations in relation to the personal data processing as set out in this Annex. In particular, it is necessary to provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of the GDPR.

8.3 With respect to each Sub-Processor, the Processor:

8.3.1. shall make every reasonable effort to verify that the Sub-Processor provides the level of personal data protection as required in the Agreement;

8.3.2. shall make sure that if the Sub-Processors are chained, the mutual rights and obligations related to personal data protection are regulated with a written agreement containing the terms and conditions granting at least the same level of personal data protection as those stated in this Amendment and/or in the Agreement, and that they comply with the requirements of Article 28 of the GDPR;

8.3.3. if personal data processing is performed by a Sub-Processor who is seated outside the EEA and, at the same time, the country where such Sub-Processor is seated was not marked by the European Commission as a country providing sufficient level of protection, the Processor has to make sure that the Processing Agreement entered into with such a Sub-Processor contains the standard contractual clauses; and

8.3.4. shall provide to the Controller upon request the copies of Processing Agreements (or similar documents) entered into with Sub-Processors which may be modified in order to eliminate confidential business information which is not relevant for the requirements of this Agreement.

8.4 The Processor has to make sure that each Sub-Processor performs the duties resulting from this Annex to the Agreement, which apply to the processing of personal data performed by such Sub-Processor as if the Processor were the party to such Agreement instead of the Processor.

8.5 The Controller is entitled to object within five working days of the notification of the need to use a new Sub-Processor that the use of a new Sub-Processor is not necessary or that the use of a new Sub-Processor entails a security risk. In this case, the Processor must prove the necessary need to use the said new Sub-Processor or propose the use of another new Sub-Processor. If the Controller finds this need justified or fails to assess the new Sub-Processor as a security risk, the Controller will allow to use the said new Sub-Processor.

9. Exercise of the Data Subject's Rights

9.1 The Processor

9.1.1. shall immediately notify the Controller, if the Processor (or any Sub-Processor) receives a request from the Data Subject aiming at the exercise of the Data Subject's Rights pursuant to the GDPR; and

9.1.2. shall make sure that the Processor (or any Sub-Processor) will not reply to requests aiming at the exercise of the Data Subject's Rights pursuant to GDPR in another way than in conformity with the Controller's written instruction and/or to the extent as required in conformity with the applicable legal regulation. In this event, however, the Processor shall notify the Controller of such a legal requirement even before the Processor (or Sub-Processor) replies to such request.

10. Personal Data Security Breach

10.1 The Processor shall inform the Controller without undue delay if the Processor or any Sub-Processor identifies a personal data security breach, and shall give sufficient information to the Controller to enable compliance with all the obligations to notify or inform the Personal Data Subject on Personal Data Security Breach pursuant to the legal regulations on personal data protection in force.

10.2 The Processor is obligated to cooperate with the Controller and to adopt the financially reasonable measures as instructed by the Controller in order to assist in investigation, mitigation and rectification of any such Personal Data Breach.

11. Destruction of Personal Data

11.1 In the event of termination of the Agreement or in the event of termination of Personal Data processing under the Agreement (hereinafter the "Termination Date"), the Processor shall immediately, but no later than within 15 days, delete all the Personal Data (including copies thereof).

11.2 The Controller may notify the Processor in writing within 5 days after the Termination Date that the Controller requests that the Processor:

11.2.1. returns all the personal data (including copies) to the Controller via secure transmission of files in a common machine-readable format; and

removes and arranges for deletion of all the other personal data (including copies) processed by any Sub-Processor. The Processor shall satisfy this written request within 10 days after the Termination Date.

11.3 Each Processor (and Sub-Processor), may, beyond the framework stipulated in the Agreement, process the Personal Data to the extent required in the relevant legal regulations, and namely only to the extent and for the period of time which is requested in such legal regulations. Furthermore, the Processor has to ensure that such Personal Data will be processed only to the extent and for the purposes mentioned in the applicable legal regulations and that they will be treated as confidential information.

11.4 The Processor shall submit to the Controller a written confirmation on compliance with the obligation related to deletion of Personal Data (including copies).

12. Inspection

12.1 The Processor shall disclose upon request any information necessary to prove compliance with this Amendment, and shall enable and shall assist at audits and inspections performed by any auditor authorized by the Controller. The Processor shall ensure such cooperation with its subcontractors.

12.2 The information rights and the rights of inspection of the processing of the Personal Data of the Controller are only established when, under the Agreement, such information is not provided to

the Controller and no rights to audit are resulting for the Controller which would comply with the requirements resulting from the applicable legal regulations (including the possible provision of Article 28, par. 3, letter h) of the GDPR).

12.3 The Controller shall notify the Processor of the inspection reasonably in advance before the Personal Data processing inspection is initiated. Furthermore, the Controller shall make reasonable efforts so that the inspection does not result in damage occurrence, excessive disturbance on the premises, of the equipment, staff and Processor's activities. The Processor is not obligated to enable access to his/her/its premises during inspection only in the event that

12.3.1. the person performing the inspection fails to submit the identity document and authorization to perform the inspection;

12.3.2. The inspection is performed outside the ordinary working hours, unless to meet its purpose, the inspection requires to be performed outside the ordinary working hours and the inspector notified the Processor in advance (during ordinary working hours) that this was such a case.