THIS AGREEMENT is made 19 day of June 2025

BETWEEN:

(1) **Total AOC Solutions Limited**, a company registered in England and Wales under number 07800710 whose registered office is at **34 Hamilton Terrace, Leamington Spa, CV32 4LY, UK** ("the Service Provider"), represented by Karl Steeves, Director; e-mail address for notices for the purpose of Clause 19: notices@trustflight.com; and

(2) **Public Institution Transport Competence Agency**, an entity registered in the Republic of Lithuania whose registered office is Rodūnios kel. 2 02189 Vilnius, legal entity code 305598608 ("the Customer"), represented by Director Marius Baranauskas, acting in accordance with the Articles of Association of the Public Institution Transport Competence Agency; e-mail address for notices for the purpose of Clause 19: info@tka.lt

(each a "Party" and "Parties" shall be construed accordingly).

WHEREAS:

(1) The Service Provider hosts and provides access to the Application described herein.

(2) The Customer wishes to access the Application described herein as hosted by the Service Provider under a non-exclusive licence, from a remote location, in return for the payment of a monthly fee and subject to the terms and conditions of this Agreement.

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Application"	means the software application provided by the Service Provider, selected Modules of which shall be available to the Customer, as set out in Schedule 1;
"ASP Infrastructure"	means the Service Provider's computer hardware, firmware, software and communications infrastructure which is used to facilitate access to the Application by the Customer;
"Business Day"	means any day which is not a Saturday, Sunday or bank or public holiday in England;
"Commencement Date"	means the latest date on which this Agreement is signed by both Parties;
"Confidential Information"	means in respect of each Party all of its business, technical, financial or other information or data disclosed to the other Party, whether during the Term or during the negotiation of this Agreement;
"Customer Computer Systems"	means the Customer's computer hardware, portable devices, firmware, software and communications infrastructure through and on which the Application are to be used;

"Customer Data"	means any data, content, material or information belonging to the Customer or to third parties and used by the Customer under licence which is created using the Application or otherwise and stored in the ASP Infrastructure;
"Data Protection Legislation"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (including all amendments);
"Domestic Law"	means the law of the United Kingdom or a part of the United Kingdom as applicable to the Service Provider;
"Legal Acts"	means legal acts of the Republic of Lithuania, European Union legal acts and international agreements, which have influence upon the implementation of this Agreement;
"Fees"	means the sums set out in Schedule 1 payable by the Customer in accordance with Clause 4;
"Intellectual Property Rights"	means all vested, contingent and future intellectual property rights, including copyright, trademarks, service marks, design rights (whether registered or unregistered), patents, know-how, trade secrets, inventions, get-up and database rights;
"Non-Customer User"	means an individual that is not a member of the Customer's organisation who shall, from time to time, access the Application through the ASP Infrastructure, but is subject to restriction as per Clause 10.3;
"Module"	means the individual parts of the Application provided by the Service Provider which the Customer has selected for use;
"Service"	means, collectively, such Modules of the Application as selected by the Customer, the ASP Infrastructure and hosting and support services provided by the Service Provider to the Customer;
"Technical Specification"	means the document attached as Annex 1;
"Term"	means the period set out in Clause 3.1 subject to earlier termination in accordance with this Agreement;
"Users"	means a member of the Customer's organisation who shall, from time to time, access the Application through the ASP Infrastructure. This includes employees, contractors and other service providers under contract with the Customer; and

"Virus" means any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

1.2 Unless the context otherwise requires, each reference in this Agreement to:

1.2.1 "writing", and any cognate expression, includes a reference to any communication effected by electronic transmission or similar means;

1.2.2 a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.3 "this Agreement" is a reference to this Agreement, each of the Schedules and Annex 1. Technical Specification;

1.2.4 a Schedule is a schedule to this Agreement;

1.2.5 an Annex is an annex to this Agreement; and

1.2.6 a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.

1.3 The terms "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "processing" and "appropriate technical and organisational measures" when used in this Agreement have meanings given in the Data Protection Legislation.

1.4 Any words following the terms "including", "include", "in particular", "for example" or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.5 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.6 Words imparting the singular number shall include the plural and vice versa.

1.7 References to any gender shall include the other gender.

2. The Service

2.1 The Service Provider shall, with effect from the Commencement Date, provide the Service to the Customer on a non-exclusive basis for the Term and in accordance with the terms and conditions of this Agreement. The Service Provider shall provide the Service with reasonable skill and care.

2.2 The Commencement Date shall be followed by an implementation phase of Self-Registration functionality for general aviation users and Desktop audits functionality allowing monitored aviation organisations to fill comments and attach evidence in questionnaire themselves while also allowing the Customer to make comments and accept or create a finding based on submitted data. Subject to performance by the Customer of its obligations and Clause 2.3 and 17, the implementation phase shall be fully completed within 12 months from the Commencement Date and consists of:

2.2.1 Configuration

2.2.2 WebEx Training (including provision to the Customer of recordings thereof)

2.2.4 Final Onsite Rollout Training (including access to online training materials as made available from time to time by the Service Provider)

2.3   The Customer shall co-operate with the Service Provider during the implementation phase and provide such access to its facilities as the Service Provider may reasonably request for such purposes.

2.4   Completion of the implementation phase shall be formalised by a service provision (transfer – acceptance) note signed by the Service Provider and the Customer. Upon receipt of the transfer – acceptance note the Customer shall sign it if the Service meets the requirements set out in the Technical Specification and the Service Provider's submitted offer. If the Service does not meet the requirements set out in the Technical Specification and the Service Provider's offer, the Customer will set in consultation with the Service Provider a reasonable time limit for the Service Provider to remedy the deficiencies.

2.5   With effect from the Commencement Date, the Service Provider shall provide access to the Application through the ASP Infrastructure and shall perform hosting services in accordance with Schedule 3 subject to the exceptions contained in Clauses 4, 8 and 17, and Schedule 3.

2.6   Other than in the provision of general support services for the Application applicable to its entire customer base, the Service Provider does not commit to making changes to the Application at the request of the Customer unless such changes are properly scoped and paid for by the Customer at a rate to be agreed between the Parties at the applicable time.

3.   Term

3.1   The Term shall commence on the Commencement Date and will continue for a period of 60 months unless terminated in accordance with this Agreement.

4.   Fees and Payment

4.1   The Fees due for the Service are specified in Schedule 1. The Fees are payable on a monthly basis. The Fees include all direct or indirect expenses of the Service Provider (except as expressly and specifically provided in this Agreement and with the exception of travel, subsistence and accommodation where on-site visits required) and costs, related to provision of the Service, including but not limited to installation, testing, start-up, error correction, improvement of the Service in accordance with the needs of the Customer, training as provided in clause 2.2, and all taxes (except, as indicated in Schedule 1, value added tax (VAT)).

4.2   Invoices will be issued by the Service Provider on a monthly basis in advance for the forthcoming month. The first invoice will be issued on the Commencement Date. The invoices must be submitted via e-mail: invoices@tka.lt. The invoices shall be submitted in euros (as set out in Schedule 1) and the payment to the Service Provider shall be made in euros via a bank transfer to the bank account indicated by the Service Provider. The invoices must include the number and the date of this Agreement.

4.3   The Customer will pay each invoice for the Fees within 30 (thirty) days of its receipt of each invoice.

4.4   If the Service commences during a month, the Service Provider will invoice the pro-rata Fees for the remainder of that month at the time it issues its next invoice, which shall be payable as provided in Clause 4.3.

4.5   If the Customer does not pay invoices in full within the time period specified in this Agreement, without prejudice to any other remedy available to it the Service Provider may suspend the Customer's use of the Service with 5 (five) Business Days' prior notice to the Customer by

removing access to the Application. Such suspension shall not relieve the Customer of any obligation to pay Fees that accrued prior to, during or after such suspension.

4.6   If the Customer does not pay invoices in full within the time period specified in this Agreement, without prejudice to Clause 4.5, at the request of the Service Provider, the Customer shall pay interest at the rate of 0,02 % of the amount not paid on time for each day of delay from the due date until payment is made in full.

4.7   This Agreement is a fixed fee (fixed price) agreement; thus, the Fees (price) of this Agreement are not subject to any adjustment throughout its entire period except in cases provided in the Law on Public Procurement of the Republic of Lithuania. Any adjustments to this Agreement price (fees) shall be made by a written agreement regarding the amendment to this Agreement duly signed by the Parties. In case there is a subsequent change in the tax legal framework applicable in Lithuania that is materially adverse to the Customer, the Customer can unilaterally terminate this Agreement by 30 (thirty) days' prior written notice to the Service Provider.

5.   The Application

5.1   The Application consists of multiple Modules. The Modules to which the Customer shall have access at the Commencement Date are detailed in Schedule 1.

6.   Training

6.1   Any additional training requested by the Customer over and above WebEx training and on-site training provided during the implementation phase referenced in Clause 2.2 may be subject to additional fees at the daily rate of €720 per day plus VAT and travel and expenses (unless otherwise agreed between the Parties) and will be subject to a separate agreement between the Service Provider and the Customer.

6.2   Following any significant change to the Application, the Service Provider shall provide the Customer with detailed release notes outlining the changes made to the system. These release notes may be delivered post-implementation of the changes. Should the Customer require training to familiarize themselves with the updates, such training shall be provided by the Service Provider subject to an additional charge as agreed between the parties.

7.   Back-Ups

7.1   The Service Provider shall make daily and monthly backups of all Customer Data. Such backups will be made shortly after 0100am UTC to data files stored on hard disks, solid state disks or similar devices.

7.2   All hard disks, solid state disks or similar devices used by the Service Provider for backups shall be stored at a site separate from the main ASP Infrastructure.

7.3   All backups made by the Service Provider will be retained for a period of one month, and the backups made by the Service Provider on the first of each month will be retained for the period of a year.

7.4   In the event of any loss or damage to Customer Data, the Service Provider shall promptly restore the lost or damaged Customer Data from the latest back-up of such Customer Data maintained by the Service Provider in accordance with the archiving procedure described in this Agreement.

7.5   Earlier backups can be restored at the Customer's request, for example for audit purposes. This will reset the system data to the time when the backup was taken.

7.6   If the Service Provider processes any Personal Data on the Customer's behalf when performing its obligations under this Agreement, the Parties record their intention that the Customer is the Controller and the Service Provider is the Processor and in any such case:

7.6.1 both Parties will comply with all applicable requirements of the Data Protection Legislation. This Clause 7.6.1 is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation;

7.6.2 Clause 7.6.6 sets out the subject matter, nature and purpose of processing by the Service Provider, the duration of the processing and the types of Personal Data and categories of Data Subject;

7.6.3 without prejudice to the generality of Clause 7.6.1, the Customer will ensure that it has a lawful basis for processing to enable lawful transfer of the Personal Data to the Service Provider for the duration and purposes of this Agreement;

7.6.4 without prejudice to the generality of Clause 7.6.1, the Service Provider shall, in relation to any Personal Data processed in connection with the performance by the Service Provider of its obligations under this Agreement:

(a) process that Personal Data only on the documented written instructions of the Customer unless the Service Provider is required by Domestic Law to otherwise process that Personal Data. Where the Service Provider is relying on Domestic Law as the basis for processing Personal Data, the Service Provider shall promptly notify the Customer of this before performing the processing required by the Domestic Law unless the Domestic Law prohibits the Service Provider from so notifying the Customer;

(b) ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(c) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

(d) other than to the Customer where the Customer is based outside of the UK, not transfer any Personal Data outside of the UK unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled: (i) the Customer or the Service Provider has provided appropriate safeguards in relation to the transfer; (ii) the Data Subject has enforceable rights and effective legal remedies; (iii) the Service Provider complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and (iv) the Service Provider complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) cooperate with the Customer in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(f) notify the Customer promptly, but not later than within 48 hours, on becoming aware of a Personal Data Breach;

(g) indicate the following information in the notification of a Personal Data Breach: the nature of the Personal Data Breach, including, where possible, the categories and approximate numbers of data subjects concerned, as well as the categories and approximate numbers of relevant personal data records; the measures taken or proposed to be taken by the Service Provider to address the Personal Data Breach, including measures to mitigate its possible adverse effects;

(h) at the written direction of the Customer, securely delete or return Personal Data and copies thereof to the Customer on termination or expiration of this Agreement unless required by Domestic Law to store the Personal Data; and

(i) maintain complete and accurate records and information to demonstrate its compliance with this Clause 7.6 and allow for audits by the Customer or the Customer's designated auditor and immediately inform the Customer if, in the opinion of the Service Provider, an instruction infringes the Data Protection Legislation;

7.6.5 the Service Provider has the right to use a third party or third parties (with Rackspace Limited and Microsoft Azure being hereby approved by the Customer) as a third-party processor of Personal Data under this Agreement as necessary in order to provide the Service, provided that the Service Provider shall inform the Customer of any intended changes concerning the addition or replacement of third party processors, thereby giving the Customer the opportunity to object to such changes. The objection/acceptance shall be received in writing from the Customer within seven (7) Business Days of its receipt of notice from the Service Provider informing it of intended changes to third party processors. The Service Provider confirms that it has entered or (as the case may be) will enter with the third-party processor into a written agreement incorporating terms which are substantially similar to those set out in this Clause 7.6. As between the Customer and the Service Provider, the Service Provider shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this Clause 7.6.5;

7.6.6 the following table sets out the subject matter, nature and purpose of processing of personal data by the Service Provider under this Agreement, the duration of the processing and the types of Personal Data and categories of Data Subject:

Subject matter: the Service Provider provides application software for use by the Customer through a system hosted and maintained by the Service Provider.

Nature: the system is a transactional system of record. The processing is automated and is of data input by or on behalf of the Customer. As a system of record the Service Provider provides storage and automated archiving of data.

Purpose: to provide operational management and support to Customer organisation.

Duration: term of this Agreement.

Categories of Data Subject: employees, customers (natural persons and representatives of legal persons) and contact persons of the Customer.

Types of Personal Data:

- name

- last name,

- telephone number,

- Email address,

- home address,
- personal code,
- date of birth,
- image,
- signature,
- a copy of the personal identity document and the personal data contained in it (name, surname, citizenship, gender, date of birth, personal code, number of the personal document (passport, identity card or similar), date of validity of the personal document, signature, photo, date of issue, place of issue),
- copy of death certificate,
- qualifications, educational attestation data, licenses, attestations, approval certificate data (number, date of issue, date of validity), examination results, ,
- bank details, bank account number,
- audio recordings (audio minutes of meetings),
- video surveillance data,
- medical certificate (EASA Medical Certificate, Driver's medical certificate or similar), date of issue, date of expiry, limitations, class,
- authorization data (data of power of attorney or similar);
- other personal data processed on legal grounds.

7.6.7. Customer-initiated additional Data Processing Agreement between The Customer and the Service Provider shall be concluded to meet the applicable requirements of The Data Protection Regulation and other legal acts.

8. Maintenance and Upgrades

8.1 The Service Provider shall be responsible in accordance with Schedule 3 for all maintenance and upgrades to the Application and ASP Infrastructure which may from time to time be required in the opinion of the Service Provider.

8.2 Subject to the provisions of Clause 11, the Customer shall be responsible for all maintenance and upgrades to the Customer Computer Systems which may from time to time be required, for example upgrades to operating systems of mobile devices, web browsers or other software used to access the Application.

8.3 The Customer acknowledges it is aware of the requirements of Schedule 2 and shall not during the Term upgrade to other software versions than those indicated in Schedule 2 without the prior consent of the Service Provider. Premature upgrade may lead to the Application being inoperable on upgraded Customer Computer Systems until the Customer downgrades to a supported version. Such a downgrade might not be possible on some devices. The Service Provider will review browser and operating system version compatibility given in Schedule 2 on an annual basis, and will give six months' advance notice in writing of changes to the list of supported browser and operating system versions, and Schedule 2 shall be deemed amended at the end of such six month period. The Service Provider will review portable device compatibility given in Schedule 2 on an annual basis, and will give 12 months' advance notice of changes to the list of supported portable devices, and Schedule 2 shall be deemed amended at the end of such 12 month period. The Customer acknowledges that failure to upgrade as

necessary may mean that it cannot access the Service, but without prejudice to its liability to pay Fees.

9. Software Licences

9.1 The Customer shall use the Application and its components under a non-exclusive, non-transferrable licence, as set out in this Agreement. The Customer shall use, and shall procure that all Users use, the Application only as expressly permitted in this Agreement.

9.2 The Service Provider warrants that the Application and its components are either its property, or that it has the requisite authority to sub-licence the Application and its components to the Customer for the purposes of this Agreement.

9.3 Nothing in this Agreement shall transfer any Intellectual Property Rights or other rights in the Application, the ASP Infrastructure or the Service to the Customer, all of which remain the property of the Service Provider or its licensors.

9.4 The Customer shall not:

9.4.1 attempt to copy, duplicate, modify, create derivative works from or distribute all or any portion of the Application except to the extent expressly set out in this Agreement or as may be allowed by any applicable law which is incapable of exclusion by agreement between the Parties;

9.4.2 store, distribute or transmit any Virus, or any material through the Service that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; facilitates illegal activity; depicts sexually explicit images; or promotes unlawful violence, discrimination based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activities;

9.4.3 attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Application, except as may be allowed by any applicable law which is incapable of exclusion by agreement between the Parties;

9.4.4 access all or any part of the Application or the Service in order to build a product or service which competes with the Application and/or the Service;

9.4.5 transfer, temporarily or permanently, any of its rights under this Agreement (except as referred to in Clause 10.4 and Clause 29.1); or

9.4.6 save in respect of Users and Non-Customer Users attempt to obtain, or assist third parties in obtaining, access to the Application and/or the Service.

10. Application and ASP Infrastructure Terms of Use

10.1 The licence granted under this Agreement, permits access for all Users authorised by the Customer at any given time.

10.2 Users' access to the Application and the ASP Infrastructure shall be controlled by means of authentication by user name and password which must be kept confidential.

10.3 Use of Non-Customer users is permitted but limited to (a) their participation in regulatory applications, (b) the filing and processing of safety reports and (c) their participation in audits and resolution of findings.

10.4 The Customer is responsible for maintaining the User's access to the Application. This includes adding and removing Users, managing User permissions, and changing User passwords. The Customer, taking all the responsibility on the Customer side, may to use functionality to authorise its clients (aviation legal entities) to administrate Non-Customer

Users, representing these entities in the limits to create, delete and manage permission of user accounts for their employees.

10.5 The Customer is exclusively responsible for its use of the Service, including the conduct of individual Users and any authorised Non-Customer Users and must ensure that all use is in accordance with this Agreement. The Customer shall notify the Service Provider immediately of any breaches of this Agreement by any Users or Non-Customer Users.

10.6 The Customer shall use, and shall procure that Users and Non-Customer Users use, the Application exclusively for the purposes of administration of processes related to the oversight of aviation entities and other activities assigned to the Customer by its Articles of Association and other Legal Acts.

10.7 The Service Provider shall monitor the Customer's, Users' and Non-Customer Users' use of the Application and ASP Infrastructure from time to time to ensure compliance with the terms and conditions of this Agreement.

10.8 The Customer, Users and Non-Customer Users may only access the Modules detailed in Schedule 1 to this Agreement. No access to other parts of the ASP Infrastructure shall be permitted in the absence of express written permission from the Service Provider.

10.9 Access to the Application is only permitted through the website tka.centrik.net.

10.10 The Customer's, Users' and Non-Customer Users' use of the Application and ASP Infrastructure may, from time to time, be governed by statutory or regulatory rules and requirements external to the terms and conditions of this Agreement. It shall be the Customer's exclusive responsibility to ensure that use of the Service is in compliance with any such laws applicable to it.

10.11 The Service provider is exclusively responsible to ensure that the provision of the Service and Application are in compliance with any laws applicable to it.

10.12 Neither the Customer, a User or Non-Customer User, nor anyone on their behalf may, in the absence of written consent from the Service Provider:

10.12.1 make changes of any kind to the Application or the ASP Infrastructure; or

10.12.2 attempt to correct any fault or perceived fault in the Application or the ASP Infrastructure.

11. Customer Computer Systems

11.1 The Customer Computer Systems shall comply with the requirements set out in Schedule 2.

11.2 The Service Provider may from time to time require physical or remote access to the Customer Computer Systems for the purposes of inspecting and testing the Customer Computer Systems to ensure their compatibility with the Application and ASP Infrastructure. Such access shall be granted by the Customer only upon receipt of reasonable notice from the Service Provider. Wherever reasonably possible, the Service Provider shall access the Customer Computer Systems using remote log-in or meeting capabilities.

11.3 Where, in the opinion of the Service Provider, Customer Computer Systems are likely to cause disruption to the ASP Infrastructure, the Service Provider may request that the Customer disconnects from the ASP Infrastructure until advised that reconnection is possible. The Service Provider may request changes such as upgrades or equipment replacement to be made to the Customer Computer Systems prior to reconnection.

11.4 The Customer shall ensure that no Customer Computer Systems interface with any third-party ASP system or other service, communications system or network in such a way that the Service may be accessed by unauthorised third parties.

12. Support

The Service Provider shall perform support services in accordance with Schedule 3 subject to the exceptions contained in Clauses 4, 8 and 17, and Schedule 3.

13. Obligations of the Parties

13.1. The Customer shall:

13.1.1 provide the Service Provider with all necessary co-operation in relation to this Agreement, and all necessary access to such information as may be required by the Service Provider, in order to render the Services, including Customer Data, security access information and software interfaces to the Customer's other business applications;

13.1.2 comply with all applicable laws and regulations with respect to its activities under this Agreement; and

13.1.3 carry out all other Customer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any undue delays in the Customer's provision of such assistance, the Service Provider may agree with the Customer to adjust any timetable as reasonably necessary.

13.2. Acting in accordance with other provisions of this Agreement (and without expanding the scope of such other provisions), the Service Provider shall:

13.2.1. provide the Service to the Customer and carry out all other Service Provider responsibilities set out in this Agreement in secure, timely and efficient manner;

13.2.2. ensure the security and confidentiality of Customer Data and Personal Data protection;

13.2.3. ensure that the Application and ASP Infrastructure may not be accessed by any unauthorised person or entity;

13.2.4. comply with all applicable laws and regulations with respect to its activities under this Agreement.

14. Customer Data

14.1 Subject to Clause 14.2 all Intellectual Property Rights subsisting in Customer Data are and shall remain the property of the Customer.

14.2 Certain Customer Data may belong to third parties. In such cases, the Customer confirms that the Customer has the right to process such data without infringing the Intellectual Property Rights of any third parties. The Service Provider acknowledges that Customer Data contains confidential information of the Customer.

15. Confidentiality

15.1 The Service Provider shall ensure that all Customer Data is kept secure and confidential.

15.2 The Service Provider shall not (and shall procure that any of it's sub-contractors and employees shall not), in the absence of prior express written consent from the Customer, disclose, transfer or in any other way make it available, Customer Data or any part thereof and any information derived from this data to any third party (other than a sub-contractor providing services to the Service Provider in respect of the Service to whom disclosure or transfer is strictly necessary for the provision of the Service) unless such disclosure is required by law or the rules of any regulator with jurisdiction over the Service Provider. In such case, where lawful to do so the Service Provider shall inform the Customer of its obligation to disclose the

Confidential information prior to such disclosure.

15.3 The Service Provider shall not (and shall procure that any of its sub-contractors and employees shall not), in the absence of prior express written consent from the Customer, access or use Customer Data for its own business purposes or any other purposes than for providing the Service to the Customer pursuant to this Agreement.

15.4 The following obligations shall apply to the Party receiving Confidential Information (the "Receiving Party") from the other Party (the "Disclosing Party").

15.5 Subject to Clause 15.6, the Receiving Party:

15.5.1 may not use any Confidential Information for any purpose other than the performance of its obligations under this Agreement;

15.5.2 may not disclose any Confidential Information to any third party except with the prior express written consent of the Disclosing Party; and

15.5.3 shall make every reasonable effort to prevent the unauthorised use or disclosure of the Confidential Information.

15.6 The obligations of confidence referred to in this Clause 15 (other than Clause 15.1) shall not apply to any Confidential Information that:

15.6.1 the Receiving Party can demonstrate it rightfully had in its possession and at its free disposal or is published or is otherwise in the public domain prior to its receipt by the Receiving Party;

15.6.2 is or becomes publicly available on a non-confidential basis through no fault of the Receiving Party or breach of this Agreement;

15.6.3 is required to be disclosed by any applicable law or regulation.

15.7 Without prejudice to any other rights or remedies the Disclosing Party may have, the Receiving Party acknowledges and agrees that in the event of breach of this Clause the Disclosing Party shall, without proof of special damage, be entitled to seek an injunction or other equitable remedy for any threatened or actual breach of the provisions of this Clause in addition to any damages or other remedies to which it may be entitled.

15.8 The obligations of the Parties under all provisions of this Clause shall survive the expiry or the termination of this Agreement irrespective of the reason for such expiry or termination.

16. Liability

16.1 This Clause 16 (except as provided in Schedule 3) sets out the entire financial liability of the Service Provider (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Customer (and any person permitted to access the Application by the Customer) arising under or in connection with this Agreement:

16.1.1 In respect of any use made by the Customer of the Application or the Service or any part of them; and

16.1.2 In respect of any representation, misrepresentation (whether innocent or negligent), statement or tortious act or omission (including negligence) arising under or in connection with this Agreement.

16.2 At the written request of the Customer, the Service Provider shall pay liquidated damages at the rate of £20 for each full working day of delay if it does not achieve any date agreed in writing for the completion of the implementation phase referenced in Clause 2.

16.3 Except as expressly and specifically provided in this Agreement:

16.3.1 the Customer assumes sole responsibility for results obtained from the use of the Application and the Service by the Customer, and for conclusions drawn from such use. The Service Provider shall have no liability for any damage caused by errors or omissions in any information, or instructions provided to the Service Provider by the Customer in connection with the Service, or any actions taken by the Service Provider at the Customer's direction; and

16.3.2 all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this Agreement.

16.4 Nothing in this Agreement excludes the liability of the Service Provider:

16.4.1 for death or personal injury caused by the Service Provider's negligence;

16.4.2 for fraud or fraudulent misrepresentation, wilfull misconduct, gross negligence or breach of Clause 15; or

16.4.3 for any other liability that cannot be excluded or limited under applicable law.

16.5 Subject to Clause 16.4:

16.5.1 neither Party shall be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation (whether innocent or negligent), restitution or otherwise for any loss of profits, loss of business, or depletion of goodwill, arising under this Agreement; and

16.5.2 the Service Provider's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement shall be limited to €120,000 (one hundred and twenty thousand euros), except in relation to breach of Clause 7.6 where the Service Provider's liability is limited to €1,500,000 (one million and five hundred thousand euros).

17. Force Majeure

Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement (other than obligations related to confidentiality of Customer Data) if such delay or failure results from events, circumstances or causes beyond its reasonable control, including strikes, lock-outs or other industrial disputes, failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, or storm. A Party shall promptly, and in any case no later than within 5 (five) Business days, notify the other Party of the *force majeure* circumstances that may prevent the fulfilment of this Agreement and of their effect on the performance of this Agreement. In case of a failure to notify the other Party within the specified period of time after the affected Party became aware, or should have become aware, of the *force majeure* event it shall not have the benefit of this Clause.

In *force majeure* circumstances the affected Party shall be entitled to a reasonable extension of the time for performing such obligations, provided that if the period of delay or non-performance continues for 90 (ninety) days, the Party not affected may terminate this Agreement by giving 30 (thirty) days' written notice to the other Party.

18. Validity, Amendment and Termination

18.1. This Agreement shall be valid until the fulfilment of the contractual obligations that are expressed to survive termination, the end of the Term or termination of this Agreement

following the procedure established under this Agreement or Legal Acts.

18.2. This Agreement may be amended during the validity period of this Agreement, provided that the conditions indicated under the Law on Public Procurement of the Republic of Lithuania are present and the principles laid down in Article 17 of the Law on Public Procurement of the Republic of Lithuania are followed. In other cases the terms of this Agreement during its validity period may not be changed. The amendments to this Agreement shall be made by written agreement of the Parties. Such agreement shall become an inseparable part of this Agreement from the day it is concluded by signature of both Parties.

18.3. This Agreement can be terminated under mutual written agreement of the Parties.

18.4 Without prejudice to any other rights or remedies to which the Parties may be entitled, either Party may terminate this Agreement without liability to the other if:

18.4.1 the other Party commits a material breach of any of the terms of this Agreement and (if such a breach is remediable) fails to remedy that breach within 30 days of that Party being notified in writing of the breach;

18.4.2 an order is made or a resolution is passed for the winding up of the other Party, or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to such other Party;

18.4.3 an order is made for the appointment of an administrator to manage the affairs, business and property of the other Party, a bankruptcy or liquidation procedure is initiated against the other Party;

18.4.4 a receiver is appointed of any of the Party's assets or undertaking, or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of such other Party, or if any other person takes possession of or sells such other Party's assets;

18.4.5 the other Party makes any arrangement or composition with its creditors, or makes an application to a court of competent jurisdiction for the protection of its creditors in any way;

18.4.6 the other Party ceases, or threatens to cease, to trade; or

18.4.7 the other Party takes or suffers any similar or analogous action to any of the foregoing in any jurisdiction applicable to it.

18.5. The Customer may terminate this Agreement without liability to the Service Provider (other than payment of sums due before and during such notice period) by giving 3 (three) months' prior notice to the Service Provider in case any authority with jurisdiction over the Customer issues a respective order or takes a respective decision, having an influence on further implementation of this Agreement.

18.6 On termination of this Agreement for any reason:

18.6.1 all licences granted under this Agreement shall immediately terminate;

18.6.2 each Party shall return and make no further use of any equipment, property, materials and other items (and all copies of them) belonging to the other Party, including Confidential Information of the other Party (provided that Customer Data shall be dealt with in accordance with Clause 18.7); and

18.6.3 the accrued rights of the Parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

18.7 The Service Provider shall make accessible for download to the Customer all Customer Data stored in the Application on the effective date of termination or expiration of this Agreement. Customer Data that was entered by the Customer (such as filled in forms, safety and quality data) will be available in XML format, and files uploaded by the Customer will be provided in the same format they were uploaded. Customer Data will be accessible for download for 90 (ninety) days from the effective date of termination, failing which the Service Provider may destroy such Customer Data after such time.

18.8 The Service Provider can provide, subject to separate fees and contract, assistance in uploading the Customer Data into other systems.

19. Notices

19.1 All notices under or in connection with this Agreement shall be in writing in the English language and shall be sent by courier or other messenger (including registered mail), by e-mail, by national ordinary mail, postage prepaid or by airmail postage prepaid.

19.2 Notices shall be deemed to have been duly given:

19.2.1 when delivered, if delivered by courier or other messenger (including registered mail) during normal business hours in the place of the recipient, or on the next commencement of normal business hours in the place of the recipient if not delivered during normal business hours in the place of the recipient; or

19.2.2 if sent by e-mail, at 9.00am on the next Business Day (where sent to the Service Provider) or the next working day of the Customer (where sent to the Customer) after transmission provided that if any e-mail produces an automated response reporting a failure to deliver, delayed delivery to the intended recipient or "out of office" reply, such e-mail shall be deemed not to have been received by the addressee;

19.2.3 on the fifth Business Day following mailing, if mailed by national ordinary mail, postage prepaid; or

19.2.4 on the tenth Business Day following mailing, if mailed by airmail, postage prepaid.

19.3 In each case notices should be addressed to the most recent address or e-mail address notified to the other Party.

19.4 In proving the giving of a notice, it shall be sufficient to prove that the notice was left or that the envelope containing the notice was properly addressed and posted, or that the applicable means of telecommunication was addressed and despatched and no automated response of the nature referenced in Clause 19.2.2 was received by the sender.

20. Relationship of Parties

Nothing in this Agreement shall create, or be deemed to create, a partnership, the relationship of principal and agent, or of employer and employee between the Service Provider and the Customer.

21. Assignment

21.1 Except as expressly provided in this Agreement, the Customer shall not assign, transfer, sub-contract, or in any other manner make over to any third party the benefit and/or burden of this Agreement without the prior written consent of the Service Provider.

21.2 If the Service Provider uses sub-contractors to perform any part of this Agreement or any specific task related to provision of the Service, the Service Provider shall remain fully responsible for the proper performance of this Agreement and fully liable for any acts or omissions of its sub-contractors, including employees and agents of its sub-contractors.

22. Severance

The Parties agree that, in the event that one or more of the provisions of this Agreement is found to be unlawful, invalid or otherwise unenforceable, that/those provisions shall be deemed severed from the remainder of this Agreement. The remainder of this Agreement shall be valid and enforceable.

23. Entire Agreement

23.1 The terms and conditions of this Agreement (including Annex 1 – Technical Specification) embody and set forth the entire agreement and understanding between the Parties and supersedes all prior oral or written agreements, understandings or arrangements relating to the subject matter of this Agreement. Neither Party shall be entitled to rely on any agreement, understanding or arrangement not expressly set forth in this Agreement, save for any representation made fraudulently.

23.2 Annex 1– Technical Specification shall form part of this Agreement. In any case of divergence or contradiction between Annex 1 – Technical Specification and the body of this Agreement or any of the Schedules, Annex 1 – Technical Specification shall prevail.

23.3 This Agreement may be varied only by a document signed by both of the Parties.

24. Third Party Rights

This Agreement does not confer any rights on any person or party (other than the Parties to this Agreement and (where applicable) their successors and permitted assigns) pursuant to legal acts.

25. No Waiver

The Parties agree that no failure by either Party to enforce the performance of any provision in this Agreement shall constitute a waiver of the right to subsequently enforce that provision or any other provision of this Agreement. Such failure shall not be deemed to be a waiver of any preceding or subsequent breach and shall not constitute a continuing waiver.

26. Marketing Rights

The Customer hereby agrees that the Service Provider may cite the Customer as a user of the Service and a customer of the Service Provider in the Service Provider's promotional and advertising literature, press releases, and in proposals and communications with customers and prospective customers. The Service Provider shall cease to cite the Customer as a customer in materials created after the end of the Term but shall not have any obligation to destroy materials already printed which it shall be entitled to distribute. The Customer may revoke marketing rights provided in this clause at any time without reasoning by giving a written notice to the Service Provider but shall not have any obligation to destroy materials already printed which it shall be entitled to distribute.

The Service Provider hereby agrees that the Customer may cite the Service Provider as a provider of services to the Customer in press releases, reports and any other material and the Customer may cite the name "Centrik" in its published (in the national registry of legal acts, website and any other public data source procedures, instructions or any other material for the Users and Non-Customer Users on the usage of the Application 27. Governing Law and Jurisdiction

27.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by and construed in accordance with the law of the Republic of Lithuania.

27.2 All the disputes, disagreements and/or claims between the Parties, arising from this Agreement or pertaining to this Agreement, implementation, termination and/or breach thereof shall be referred to negotiation between the Parties. The negotiations shall be deemed to begin on the day when one of the Parties submits a written request to the other Party to start

negotiations.

27.3. In case the Parties fail to solve the dispute pertaining to this Agreement by bilateral negotiations in 30 days, the dispute shall be referred to and finally solved by the courts of the Republic of Lithuania following the procedure established under the laws of the Republic of Lithuania.

28. Persons, responsible for the implementation of this Agreement

28.1. Persons responsible for the implementation of this Agreement and operational communication focal points:

28.1.1 Customer representatives – Vidmantas Plėta, Civil aviation department director, e.mail vidmantas.pleta@tka.lt and Vitalijus Krivoščenko, chief specialist of Airworthiness division, e.mail vitalijus.krivoscenko@tka.lt.

28.1.2 Service Provider representative: to be notified.

28.2. Persons responsible for the implementation of this Agreement and their contacts may be changed by written notice given to the other Party.

29. Final provisions

29.1. The Customer shall be entitled without a separate written consent of the Service Provider to transfer the rights and obligations established under this Agreement to other legal person of any form, which takes over the rights and obligations of the Customer in case of reorganisation and (or) restructuring of the Customer in accordance with the procedure established under the Legal Acts. The Customer shall notify the Service Provider on the transfer of rights and liabilities to another legal person not later than within 20 (twenty) Business Days after the transfer of the rights and obligations.

29.2. This Agreement has been concluded in two copies of the same legal power, one for each of the Parties.

30. Legal contact data of the Parties

The Customer	The Service Provider
Public institution Transport Competence Agency Legal entity code: 305598608 VAT code: LT100013737411 Registered office at: Rodūnios road 2, LT-02189 Vilnius Tel.: +370 5 2739038 Email address: info@tka.lt Settlement account number: LT417044090100712664 Bank: AB SEB bankas, bank code: 70440	**Total AOC Solutions Limited** Legal entity code: 07800710 Registered office at: 34 Hamilton Terrace, Leamington Spa, CV32 4LY, UK Email address: accounts@trustflight.com Bank Account Details: Account No: 86615582 Sort Code: 30-90-57 Account Details: Current Account Euro BIC: LOYDGB21193 IBAN: GB27 LOYD 3090 5786 6155 82
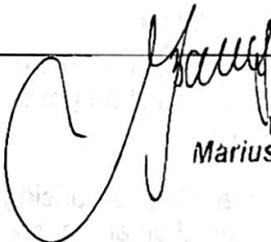
Direktorius
Marius Baranauskas

J KARL STREVES
DIRECTOR

SCHEDULE 1

Modules available at Commencement Date

Modules	
Forms	Equipment
Contacts	Action Management
Personalised Dashboard	Documents / EFB
Risk	Standard Training
Meetings	Workflows
Regulator Oversight	Aircraft Registry
Reporting (Safety)	Internal QA (Compliance)
Regulations	Regulator Application Module
Registry Module	

System
Centrik for Regulators

Functionality or modules to be available after Commencement date

Functionality	To be available by
Desktop audits functionality allowing monitored aviation organisations to fill comments and attach evidence in questionnaire themselves while also allowing the Customer to make comments and accept or create a finding based on submitted data	12 months after Commencement Date
Self Registration external users.	12 months upon request by the Customer

Fees:

Description	Price
Centrik system to include modules listed above	5750 € per month
WebEx Setup and Implementation	Free of Charge
Travel and Expenses	Charged at Cost (agreed prior with the Customer)

All fees and rates stated are in EUR per calendar month, and are exclusive of VAT (if applicable).

€720 per day daily rate for additional works after initial training and time spent providing additional services or maintenance and support not included within Schedule 3 (including in relation to matters set out in paragraph 3 of Schedule 3) and provided at request of the Customer (charged in units of 1 hour (calculated upwards in respect of part hours)) and calculated pro rata to the day rate referenced (7 hour day)).

Total AOC Solutions Ltd   Application Service Agreement   19

SCHEDULE 2

System Requirements / Compatibility

Desktop Browsers
Google Chrome – version 70 upwards
Apple Safari – version 12 upwards
Microsoft Edge – version 80 upwards

Portable Devices
Apple iPad – iOS 13 upwards
Android tablets – Android 10 upwards

SCHEDULE 3

1. MAINTENANCE EVENTS

Maintenance of the ASP Infrastructure, Application or other aspects of the Service that may require interruption of the Service (**Maintenance Events**) shall not be performed during Normal Business Hours (06.00am to 23.00pm local UK time, each Business Day) unless the Service Provider gives the Customer no less than 48 hours' prior notice. The Service Provider may interrupt the Service to perform emergency maintenance during the daily window of 23.00 pm to 02.00am UK time. Any Maintenance Events that occur during Normal Business Hours, and which were not requested or caused by, or notified as referenced above in advance to, the Customer, shall be considered downtime for the purpose of service availability measurement. The Service Provider shall at all times use reasonable endeavours to keep any service interruptions to a minimum.

2. MAINTENANCE

2.1 Maintenance includes all regularly scheduled error corrections to the Application.

2.2 The Service Provider shall maintain the Application and the ASP Infrastructure. Should the Customer determine that the Application or the ASP Infrastructure includes a defect, the Customer may at any time file error reports and the Service Provider shall use reasonable commercial endeavours promptly to correct any errors. During maintenance periods, the Service Provider may, at its discretion, upgrade versions, install error corrections and apply patches to the Application and the ASP Infrastructure. The Service Provider shall use reasonable commercial endeavours to avoid unscheduled downtime for Application and ASP Infrastructure maintenance.

3. TECHNICAL SUPPORT SERVICES

3.1 The Service Provider shall provide the Customer with technical support services. The Customer shall notify in writing to the Service Provider up to a maximum of 5 personnel to act as Internal Centrik Administrators (**ICA**) who shall be authorised to contact the Service Provider for technical support services. The Service Provider shall provide technical support services only to such specified ICA's.

3.2 The ICA's are given access to Centrik Support 365 days per year via:

(a) Telephone: +44 (0) 1959 543 204

(b) Email: Support@Centrik.net

(c) Customer Centrik System Support Request Function

(d) Access to Customer Support Ticket Portal: Zendesk

The Service Provider technical support call centre shall respond to all support requests from ICA's within the time periods specified below, according to priority

3.3 The named ICA's and Centrik Support shall jointly determine the priority of any defect, using one of following priorities:

Severity	Definition	Response Time *	Resolution Time
Critical	Complete outage of system or serious degradation impacting at least 80% of users	30 minutes	2 hours
High	Limited degradation of system preventing use of key features and impacting at least 20% of users E. g. Users are unable to submit reports	1 hour	1 working day

Medium	Recurring defects affecting localised features that do not meet the criteria above E.g. Managers are unable to filter KPI report as desired	2 hours	1 week
Low	Minor defects that do not prevent effective usage of the system, or have ready workarounds	1 day	No commitment

* During support hours 24/7; 365 days per year

3.4 If no response has been received on a Priority 1 or Priority 2 incident within the relevant response time specified in the table set out in paragraph 3.3, the incident shall be escalated to the Service Provider's key personnel, details of which will be provided to the Customer from time to time or on request.

Service Level Arrangements

1. **AVAILABILITY**

   Subject to the exceptions contained in Clauses 4, 8 and 17, and Schedule 3, the Service Provider shall provide at least a 99.9% uptime service availability level (**Uptime Service Level**). Downtime in this context refers to an unplanned Priority 1 defect as defined in the table set out in paragraph 3.3 of Schedule 3 or a Maintenance Event that was not notified to the Customer in accordance with paragraph 1 of Schedule 3.

2. **AVAILABILITY MEASUREMENT**

   The availability measurement is based on the monthly average percentage availability, calculated at the end of each calendar month as the total actual uptime minutes divided by total possible uptime minutes in the month. The Service Provider shall keep and shall send to the Customer, on request, full records of its availability measurement activities under this Agreement.

3. **SERVICE CREDITS**

3.1 If availability falls below the Uptime Service Level in a given calendar month (**Service Delivery Failure**), the Service Provider shall credit the Customer's account by an amount calculated as the product of the total cumulative downtime (expressed as a percentage of the total possible uptime minutes in the month concerned) and the total Fee for that month (**Service Credit**).

3.2 The maximum Service Credit allowable in a given month is limited to an amount equal to 100% of the total Fee for that month.

3.3 The Customer acknowledges and agrees that Service Credits constitute a genuine pre-estimate of the loss or damage that the Customer would suffer as a result of the Service Provider's Service Delivery Failure and are not intended to operate as a penalty for the Service Provider's non-performance. The Customer further acknowledges and agrees that payment of Service Credits constitutes the Customer's exclusive remedy in respect of the Service Provider's Service Delivery Failure.

3.4 Sums paid as Service Credits to the Customer shall count towards the Service Provider's cap on its liability in Clause 16.4.2.

IN WITNESS WHEREOF this Agreement has been duly executed the day and year first before written

....

Karl Steeves, Director
for and on behalf of Total AOC Solutions Limited

....
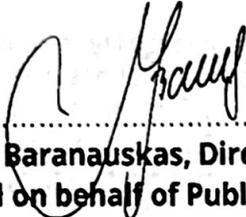
Marius Baranauskas, Director
For and on behalf of Public Institution Transport Competence Agency.

ANNEX 1

TECHNICAL SPECIFICATION
TECHNINĖ SPECIFIKACIJA

AVIACIJOS PRIEŽIŪROS SISTEMA
THE AVIATION SURVEILLANCE SYSTEM

Pirkėjas – viešoji įstaiga Transporto kompetencijų agentūra./
The Buyer – Public Enterprise Transport Competence Agency.

Tiekėjas – konkurso laimėtojas, su kuriuo Pirkėjas sudarys viešojo pirkimo-pardavimo sutartį./
The Supplier – the winner of the tender, with which the Buyer will conclude a public purchase-sale agreement.

Pirkimo objektas – programinės įrangos pagrindu sukurtas įrankis, skirtas administruoti su aviacijos subjektų priežiūra susijusius procesus, apibendrintai vadinamas aviacijos priežiūros sistema. Pirkimo objektas turi atitikti visus žemiau išvardintus reikalavimus./
Procurement object – a software-based tool for the administration of processes related to the oversight of aviation entities, collectively referred to as the aviation surveillance system. The procurement object must meet all the requirements listed below.

Pirkimo objektui keliami reikalavimai	Requirements for the object of procurement
1. Aviacijos priežiūros sistema (toliau – Sistema) turi suteikti galimybę atlikti žemiau išvardytas užduotis:	1. The aviation surveillance system (System) shall be capable of performing the following tasks:
1.1. Ūkio subjektų priežiūros užduotys:	1.1. Supervision tasks of entities:
1.1.1. Sistema privalo turėti bendrosios informacijos apie ūkio subjektus (ir kitus klientus) duomenų bazę.	1.1.1. The system must have a database of general information about entities (and other customers).
1.1.2. Yra galimybė sudaryti kelis vienas nuo kito nepriklausomus Audito planus ir juos modifikuoti. Galimas audito plano tvarkaraščio sudarymas iki 4 metų, mažiausiai 2 metai į priekį.	1.1.2. Creation/modification of audit plans - audit plan schedule vision to the 4 next years (2 years minimum).
1.1.3. Yra galimybė atlikti ūkio subjektų rizikingumo vertinimą atsižvelgiant į įmonės rizikos vertinimo modelį.	1.1.3. Possibility to perform a risk assessment of entities based on specific risk assessment model.
1.1.4. Yra galimybė atlikti ūkio subjektų priežiūros klausimynų rengimą, peržiūrą ir pildymą.	1.1.4. Possibility to prepare, review and fill in the audit questionnaires / checklists.
1.1.5. Sistema leidžia atlikti prižiūrimų ūkio subjektų auditų vykdymo priskyrimą konkretiems auditoriams su galimybe perskirstyti auditus tarp auditorių.	1.1.5. System can keep several independent audit programmes, performed on an individual schedule, which can be flexibly assigned (and re-assigned) to auditors.
1.1.6. Yra galimybė ūkio subjektų priežiūros ataskaitą pateikti ūkio subjektui, atlikti ištaisomųjų veiksmų plano suderinimą, atlikti įgyvendintų ištaisomųjų veiksmų įrodymų pateikimą ir saugojimą bei kitos su trūkumų ištaisymų susijusios informacijos pateikimą bei saugojimą.	1.1.6. Possibility to submit an audit report to the entity, to coordinate the corrective action plan, to provide and store evidence of the implemented corrective actions and provide and store other information related to the rectification of deficiencies.
1.1.7. Yra galimybė atlikti audituojamo ūkio subjekto įtraukimą kaip išorinio vartotojo, leidžiant sukurti auditą būtent šiam subjektui. Sistema suteikia galimybę informuoti tikrinamą	1.1.7. Audited entities can be set up as external users, allowing you to create the audit specifically for that entity. The audited entity will be informed of the planned audit, any findings will be automatically assigned to designated contacts within the audited organisation/entity and you will have complete oversight of their response and deficiency mitigation actions.
	1.1.8. The system should be setup in a way to make a clear difference between internal and external auditees.

Pirkimo objektui keliami reikalavimai	Requirements for the object of procurement
subjektą apie planuojamą auditą, automatiškai pateikti išvadas priskirtos audituojamos organizacijos paskirtiems kontaktams su galimybe peržiūrėti jų atsakymus ir su trūkumų ištaisymų susijusią informaciją. 1.1.8. Sistema turi būti sukonfigūruota taip, kad būtų aiškus skirtumas tarp vidinių ir išorinių audituojamų subjektų. 1.1.9. Yra galimybė filtruoti auditus pagal audito savininkus ir audituojamą subjektą, audito sritį. 1.1.10. Sistema leidžia prižiūrėti kiekvieną organizaciją per atskirą informacijos suvestinę, kurioje yra skyrius patvirtinimams ir sertifikatams.	1.1.9. Ability to filter audits per audit owner, auditee and area. 1.1.10. Ability to manage each organisation via a standalone dashboard which includes a section for approvals and certificates.
1.2. Dokumentų valdymas ir saugojimas: 1.2.1. Sistemoje turi būti TKA priežiūros veikloje naudojamų ES teisės aktų/ reglamentų bazė. 1.2.2. Sistemoje turi būti TKA vidaus dokumentų (tvarkų, procedūrų) bazė. 1.2.3. Yra galimybė platinti dokumentus ir kitus pranešimus darbuotojams bei užtikrinti, kad jie būtų gaunami ir perskaityti. 1.2.4. Yra galimybė elektroniniu būdu pasirašyti (angl. *sign off*) ataskaitas ir kitus dokumentus. 1.2.5. Sistema turi leisti apriboti vartotojams prieigą prie konkrečių duomenų, nesusijusių su atitinkamo vartotojo prieigos teisėmis. 1.2.6. Sistemoje suteikiama užduočių valdymo galimybė su veiksmo priskyrimu darbuotojui, veiksmų atlikimo seka, galimybe patvirtinti, kad veiksmai iš tikrųjų buvo atlikti ir galimybe pabaigti darbų seką. Taip pat yra galimybė deleguoti veiksmus. 1.2.7. Yra galimybė platinti dokumentus ir kitus pranešimus išorės vartotojams ir užtikrinti, kad jie būtų gaunami ir perskaityti.	**1.2. Document management and storage:** 1.2.1. System must have database of EU legislation / regulations used in TKA oversight activities. 1.2.2. System must have database of TKA internal documents (procedures). 1.2.3. Ability to distribute documents and other communications to staff, and ensure they are received and read. 1.2.4. Ability to sign-off reports and other documents electronically. 1.2.5. The system should be able to restrict the access to specific data in relation to the access rights/authority of the relevant user. 1.2.6. Tasks can be created and follow a clear workflow - from assigning the action task to an individual to performing the task with the ability to confirm that the action has indeed been performed and can be closed. Actions can also be delegated. 1.2.7. Ability to distribute documents and other communications to external entities, and ensure they are received and read.
1.3. Rizikos valdymo užduotys: 1.3.1. Sistema privalo turėti TKA veiklos grėsmių ir rizikų registrą. 1.3.2. Sistema privalo turėti dvi ar daugiau modifikuojamos rizikos valdymo metodologijas, kurios analizuotų pavojaus pasekmes pagal tikimybę ir sunkumą. 1.3.3. Sistema turi sugebėti tvarkyti ir saugoti pokyčių valdymo formas ir duomenis. 1.3.4. Sistema turi gebėti apibrėžti ir stebėti didžiausią riziką, sugebėti sukurti kelis rizikos registrus.	**1.3. Risk management tasks:** 1.3.1. The software must have risk and hazard register. 1.3.2. The system must be able to provide multiple modifiable / definable risk methodologies, which would analyse the consequences of the hazard in terms of probability and severity. 1.3.3. The system must be able to manage and store change management forms and data. 1.3.4. The system must ability to define and monitor top risks, ability to create multiple risk registers
1.4. Pranešimų apie civilinės aviacijos įvykius analizė: 1.4.1. Turi būti iš ūkio subjektų ir privačių asmenų gaunamų saugos pranešimų duomenų bazė. 1.4.2. Yra galimybė sukurti modifikuojamą elektroninę pranešimų teikimo sistemą, kuri	**1.4. Analysis of civil aviation occurrence reports:** 1.4.1. System must have database of safety occurrence reports received from entities and private persons. 1.4.2. Possibility to develop a modifiable electronic reporting system that would generate a report in a format compatible with the ECCAIRS (European Coordination Center for Accident and Incident

Pirkimo objektui keliami reikalavimai	Requirements for the object of procurement
suformuotų pranešimą formatu suderinamu su ECCAIRS (European Co-ordination Centre for Accident and Incident Reporting Systems) ir ADREP (The Accident/Incident Data Reporting) taksonomija ir atitiktų Europos Parlamento ir Tarybos reglamento (ES) Nr. 376/2014 keliamus reikalavimus.	Reporting Systems) and ADREP (The Accident / Incident Data Reporting) taxonomy and comply with Regulation (EU) No. 376/2014 of the European Parliament and of the Council.
1.4.3. Sistema leidžia atlikti saugos pranešimo apie įvykius rizikos įvertinimą bei papildomos informacijos prie pranešimo įrašo suvedimą.	1.4.3. The system allows performing a risk assessment of the safety occurrence reporting and entering additional information to the report.
1.4.4. Sistema turi leisti vartotojams kurti ir siųsti konfidencialius pranešimus (nerodant vardų).	1.4.4. The system must allow users to create and send confidential messages (without displaying names).
1.4.5. Sistema turi leisti vartotojams sudaryti ERC (Event Risk Classification) įvykių rizikos klasifikavimo įvertinimą.	1.4.5. The system must allow users to produce an ERC (Event Risk Classification) score.
1.4.6. Sistema turi leisti vartotojams sudaryti ERCS (European risk classification scheme) įvykių rizikos klasifikavimo įvertinimą	1.4.6. The system must allow users to produce an ERCS (European risk classification scheme) score.
1.4.7. Sistema turi sugebėti automatiškai parengti metriką, KIP ir statistinius duomenis iš pranešimų sistemos ir atitikties stebėsenos duomenų	1.4.7. The system must be able to produce metrics, KIPs and statistical data automatically from the reporting and compliance data in the system
1.5. Atitikties valdymas:	**1.5. Compliance monitoring:**
1.5.1. Sistema leidžia atlikti vidaus auditų plano rengimą.	1.5.1. The system allows the development of an internal audit plan.
1.5.2. Sistema leidžia atlikti vidaus auditų klausimyno rengimą, peržiūrą ir pildymą.	1.5.2. Possibility to prepare, review and fill in the internal audit questionnaires / checklists.
1.5.3. Yra galimybė parengti audito ataskaitas, ištaisomųjų veiksmų plano suderinimą, įgyvendintų ištaisomųjų veiksmų įrodymų pateikimą ir saugojimą bei kitos su trūkumų ištaisymų susijusios informacijos pateikimą bei saugojimą.	1.5.3. There is an opportunity to prepare audit reports, coordination of corrective action plan, provide and store evidence of implemented corrective actions, and provide and store other information related to corrective actions.
1.5.4. Sistema užtikrina vidaus audito atlikimą bei komunikaciją su už trūkumų ištaisymą atsakingu darbuotoju.	1.5.4. The system ensures the performance of internal audit and communication with the employee responsible for findings.
1.5.5. Sistema gali suskurti automatinį pranešimą / informaciją darbuotojams apie jiems priskirtų neatitikčių statusą.	1.5.5. The system can generate an automatic notification / information to employees about the status of non-compliances assigned to them.
1.5.6. Yra galimybė stebėti pasirenkamus KPI (angl. *Key performance indicators*) pažangos rodiklius.	1.5.6. System can track progress of KPI (Key performance indicators) against targets.
1.6. Orlaivių tinkamumas skraidyti:	**1.6. Airworthiness tasks:**
1.6.1. Sistemoje galima orlaivių klasifikacija pagal tipą, modelį ir gamintoją. Naudojantis ADREP taksonomija.	1.6.1. The system allows the classification of aircraft by type, model and manufacturer. Using embedded ADREP taxonomy.
1.6.2. Yra galimybė valdyti orlaivio tipo pažymėjimus ir papildomus tipo pažymėjimus bei jų turėtojus.	1.6.2. System provides the ability to manage aircraft type certificates and supplemental type certificates and holders.
1.6.3. Yra galimybė valdyti tinkamumo skraidyti patikrą ir jos laikymąsi.	1.6.3. Ability to manage the applicability and compliance with airworthiness review.
1.6.4. Yra galimybė sudaryti ir valdyti orlaivių dokumentų registrą.	1.6.4. Ability to create and manage aircraft documentation register.
1.6.5. Yra galimybė valdyti orlaivių registracijos numerių paskirstymą, savininkų ir patikrų įrašus.	

Pirkimo objektui keliami reikalavimai	Requirements for the object of procurement
	1.6.5. System provides the ability to manage allocation of aircraft registration numbers, owners, and inspection records.
1.7. Mokymų valdymas:	**1.7. Training management:**
1.7.1. Yra galimybė nustatyti mokymų / kvalifikacijos reikalavimus atskiroms funkcijoms.	1.7.1. It is possible to set training / qualification requirements for individual functions.
1.7.2. Yra galimybė užfiksuoti ir saugoti atliktų mokymų dokumentus.	1.7.2. It is possible to record and store documents of completed training.
1.7.3. Sistema leidžia stebėti kvalifikacijos / mokymų galiojimo laiką ir automatiškai informuoti apie mokymo kvalifikacijos artėjimą prie pabaigos.	1.7.3. The system allows to monitor the validity period of the qualification / training and automatically informs about the approach of the training qualification to the expiry.
1.7.4. Yra galimybė automatiškai nustatyti mokymų / kvalifikacijos reikalavimus pagal priskirtas funkcijas, stebėti ir pažymėti, kai mokymų / kvalifikacijos galiojimas pasibaigia.	1.7.4. It is possible to set training / qualification requirements automatically according to the assigned functions; monitor and mark when the training / qualification expires.
1.8. Papildomi funkcionalumai:	**1.8. Additional functionality:**
1.8.1. Galimybė kurti ir tvarkyti paraiškų formas;	1.8.1. Ability for the public institution Transport Competence Agency (hereinafter in this Technical Specification – TKA) to create and manage application forms;
1.8.2. Prieiga TKA klientams pateikti paraiškos formas:	1.8.2. Access for TKA clients to submit application forms:
1.8.2.1. užpildyti ir pateikti paraišką bei prie jos pridedamus dokumentus;	1.8.2.1. fill out and submit an application and related documentation;
1.8.2.2. komunikuoti su inspektoriumi dėl kiekvienos paraiškos;	1.8.2.2. communicate with the inspector regarding each application;
1.8.2.3. pateikti dokumentus paraiškos vertinimo proceso metu;	1.8.2.3. submit documents during the application evaluation process;
1.8.2.4. TKA klientui atsisiųsti išduotus dokumentus;	1.8.2.4. download documents issued to TKA client;
1.8.3. Galimybė TKA apdoroti paraiškas:	1.8.3. Ability for TKA to process applications:
1.8.3.1. vertinti paraišką naudojant darbo eigos modulį paraiškų modulyje;	1.8.3.1. evaluate the application using the workflow module in the applications module;
1.8.3.2. komunikuoti su TKA klientais dėl kiekvienos paraiškos ;	1.8.3.2. communicate with the TKA client regarding each application;
1.8.3.3. patvirtinti paraišką;	1.8.3.3. approve an application.
1.8.4. Sertifikato generavimas:	1.8.4. Generation of Certificate:
1.8.4.1. galimybė TKA generuoti ir išduoti sertifikatus;	1.8.4.1. ability for TKA to generate and issue certificates;
1.8.5. Registro funkcijos:	1.8.5. Registry functions:
1.8.5.1. registruoti paraiškas ir sertifikatus registruose, suteikti unikalius numerius;	1.8.5.1. register applications and certificates in registers, assign unique numbers;
1.8.5.2. sudaryti ir valdyti orlaivių, licencijų ar kitų tipų registrus;	1.8.5.2. create and manage aircraft, license or other types of registers;
1.8.5.3. sudaryti ir valdyti su paraiškų moduliu nesusijusius registrus;	1.8.5.3. create and manage registers not related to the application module;
1.8.6. Sistema turi siųsti ūkio subjektui pranešimus apie:	1.8.6. The system shall send notifications to TKA clients on:
1.8.6.1. pasikeitimus vertinimo ir tvirtinimo procese;	1.8.6.1. changes in application evaluation and approval process;
1.8.6.2. naujus inspektoriaus komentarus;	1.8.6.2. new inspector comments;
1.8.6.3. proceso užbaigimą ir informaciją apie išduotus sertifikatus;	1.8.6.3. end of process and information on issued certificates;
1.8.7. Galimybe bendrosios aviacijos subjektui susikurti paskyrą ir gauti prieigą, leidžiančią teikti paraiškas paraiškų modulyje;	

Pirkimo objektui keliami reikalavimai	Requirements for the object of procurement
1.8.8. Galimybe atlikti nuotolinius auditus (angl. Desktop Audits), kai ūkio subjektai nuotoliniu būdu, naudojant suteiktą paskyrą, užpildo komentarus ir/ar prideda įrodymus (dokumentą, foto ar video medžiagą), o TKA atstovas priima pateiktą informaciją arba nustato trūkumą pagal pateiktą informaciją; 1.8.9. Programos sąsaja paraiškų modulyje, susiejanti paraiškų modulį su mokėjimų administravimu išorinėje sistemoje.	1.8.7. With the possibility for a general aviation entity to create an account and obtain access allowing to submit applications in the application module; 1.8.8. With the possibility of conducting remote audits (Desktop Audits), when business entities remotely, using the provided account, fill in comments and/or add evidence (document, photo or video material), and TKA representative accepts the provided information or raises a finding based on the provided information; 1.8.9. Application program interface in the application module allowing to exchange information between applications module and administration of payments in an external system.
2. Sistema turi atitikti šiuos techninius reikalavimus:	2. The System must meet the following specifications:
2.1. Sistemos licencijavimo ir pateikimo klientui modelis – programinė įranga TKA pateikiama kaip paslauga (angl. Software-as-a-Service – SaaS).	2.1. Software licensing and delivery model must be „Software-as-a-Service – SaaS" where Supplier provides system as service that is hosted on its own infrastructure.
2.2. Tiekėjas turi suteikti techninę pagalbą vartotojui (angl. User support): 2.2.1. Tiekėjas privalo teikti nepertraukiamo techninio palaikymo paslaugą (24/7/365). 2.2.2. Kvalifikuota techninė pagalba turi būti teikiama kreipiantis telefonu, elektroniniu paštu ir kitomis ryšio priemonėmis.	2.2. Supplier must provide user support: 2.2.1. Supplier must provide continuous user support (24/7/365). 2.2.2. User support must be provided over the phone, email, or other means of communication.
2.3. Siekiant užtikrinti sklandų Sistemos veikimą, tiekėjas nuolat vykdo programinės įrangos veikimo stebėseną ir atlieka gedimų šalinimą. Tiekėjas privalo nuolat stebėti ir pateikti įrodymus: 2.3.1. Web aplikacijos neatsiliepimus (angl. Web application unresponsiveness); 2.3.2. Aplikacijos konfigūravimo klaidas; 2.3.3. Atsarginių kopijų būklę; 2.3.4. Atsarginių kopijų klaidas; 2.3.5. DNS įvesties klaidas; 2.3.6. Elektroninių laiškų siuntimo būklę; 2.3.7. Duomenų bazės versijų (angl. versioning) klaidas.	2.3. In order to ensure the smooth operation of the system Supplier constantly carries out monitoring of the operation of software and performs troubleshooting. The Supplier must constantly monitor and be able to evidence: 2.3.1. Web application unresponsiveness; 2.3.2. Software environment configuration errors; 2.3.3. Data backup status; 2.3.4. Data backup errors; 2.3.5. DNS entry errors; 2.3.6. Email sending status; 2.3.7. Database versioning problems.
2.4. Tiekėjas įsipareigoja vykdyti programinės įrangos atnaujinimus.	2.4. The Supplier undertakes to perform software updates.
2.5. Tiekėjas įsipareigoja talpinti Sistemos programinę įrangą ir duomenų bazę didelio pasiekiamumo (angl. high-availability) serveriuose, kurie turi būti saugomi bent dviejuose duomenų centruose, esančiuose skirtingose geografinėse vietovėse.	2.5. The Supplier undertakes to host the System software and database on high-availability servers, which must be stored in at least two data centers located in different geographical areas.
2.6. Siekiant užtikrinti sklandų Sistemos veikimą, tiekėjas nuolat vykdo infrastruktūros stebėseną. Tiekėjas privalo nuolat stebėti: 2.6.1. Virtualios mašinos ir hipervizoriaus resursų būklę; 2.6.2. Tinklo būklę;	2.6. In order to ensure the smooth operation of the System, the Supplier shall continuously monitor the infrastructure. The Supplier must constantly monitor: 2.6.1. Virtual machine and hypervisor resource utilization; 2.6.2. Network status;

Pirkimo objektui keliami reikalavimai	Requirements for the object of procurement
2.6.3. PING parametrą; 2.6.4. SQL serverio ryšio būklę; 2.6.5. HTTP/HTTPS būklę; 2.6.6. DNS būklę.	2.6.3. Ping monitoring; 2.6.4. SQL server connection status; 2.6.5. HTTP/HTTPS status checks; 2.6.6. DNS status.
2.7. Tiekėjas įsipareigoja kasdien bei kas mėnesį daryti atsargines duomenų kopijas: 2.7.1. Dienos kopijos turi būti saugomos ne trumpiau kaip 1 mėnesį. 2.7.2. Mėnesio kopijos turi būti saugomos ne trumpiau kaip 12 mėnesių.	**2.7. The Supplier undertakes to make daily and monthly backups of data:** 2.7.1. Daily copies must be kept for at least 1 month. 2.7.2. Monthly copies must be kept for at least 12 months.
2.8. Tiekėjas užtikrina Sistemos pasiekiamumą šiomis priemonėmis: 2.8.1. Darbui su Sistema tinkamos Blink, Webkit, Gecko arba lygiaverčius variklius turinčios interneto naršyklės. 2.8.2. Darbui su Sistema tinkamos Windows, OSX, Android, iOS arba lygiavertės operacinės sistemos.	**2.8. Supplier shall ensure access to the system with:** 2.8.1. Web browsers with Blink, Webkit, Gecko or equivalent engines; 2.8.2. Windows, OSX, Android, iOS or equivalent operating systems.
2.9. Reikalavimai užtikrinantys kibernetinę saugą: 2.9.1. Tiekėjas turi pateikti sertifikatus patvirtinančius standartų įdiegimą: 2.9.2. ISO 9001 arba lygiaverčio kokybės kontrolės standarto (angl. Quality Management); 2.9.3. ISO 27001 arba lygiaverčio informacijos saugumo standarto (angl. Information Security). 2.9.4. Turi būti atliekamas duomenų saugykloje saugomų duomenų šifravimas (angl. Data at Rest Encryption). 2.9.5. Tiekėjas turi periodiškai, ne rečiau kaip kasmet, organizuoti kibernetinės saugos testus – bent įsiskverbimo testavimą (angl. penetration testing); 2.9.6. Sistema turi atitikti Bendrojo duomenų apsaugos reglamento (BDAR) reikalavimus. 2.9.7. Vartotojų autentifikavimas turi būti vykdomas panaudojant aktyvių katalogų sistemą „Microsoft Active Directory" arba dviejų žingsnių tikrinimą (angl. two step verification). 2.9.8. Turi būti naudojama žiniatinklio aplikacijų ugniasienė (angl. Web Application Firewall (WAF)); 2.9.9. Turi būti naudojama antivirusinė programinė įranga ir atakų prevencijos sistema (angl. host intrusion prevension system (HIPS)); 2.9.10. Duomenų perdavimui turi būti naudojamas saugus duomenų perdavimo protokolas – TLS (angl. Transport Layer Security) arba lygiavertis; 2.9.11. TKA duomenys turi būti saugojami atskirai nuo kitų Tiekėjo klientų duomenų.	**2.9. Requirements to ensure cyber security:** 2.9.1. The Supplier must provide certificates confirming the implementation of the standards: 2.9.2. ISO 9001 „Quality Management" or equivalent quality control standard; 2.9.3. ISO 27001 „Information Security" or equivalent information security standard; 2.9.4. Data on storage must be kept encrypted (Data at Rest Encryption); 2.9.5. The Supplier must periodically, at least annually, organize cyber security tests - at least penetration testing; 2.9.6. The system must comply with the requirements of the Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). 2.9.7. User authentication must be performed using Microsoft Active Directory or two step verification. 2.9.8. Web Application Firewall (WAF) must be used; 2.9.9. Antivirus software and host intrusion prevention system (HIPS) must be used; 2.9.10. A secure data transmission protocol - TLS (Transport Layer Security) or equivalent - must be used for data transmission; 2.9.11. TKA data must be stored separately from other Supplier's customer data.

Pirkimo objektul kellaml reikalavimai	Requirements for the object of procurement
2.10. Duomenų valdymas: 2.10.1. Tiekėjas užtikrina galimybę TKA atsisiųsti duomenis į savo infrastruktūrą naudojant SFTP (angl. Secure File Transfer Protocol) arba lygiavertį saugaus failų perdavimo protokolą; 2.10.2. Tiekėjas įsipareigoja suteikti bandomąją Sistemos versiją (bandymų atlikimui naudojamos Sistemos atvaizdas).	**2.10. Data management:** 2.10.1. The Supplier shall ensure the possibility for the TKA to download data to its infrastructure using SFTP (Secure File Transfer Protocol) or an equivalent secure file transfer protocol; 2.10.2. The Supplier undertakes to provide a trial version of the System (image of the System used for testing).
3. Reikalavimai mokymų sesijai: 3.1. Po kiekvieno esminio sistemos pasikeitimo tiekėjas įsipareigoja supažindinti pirkėją su pakeitimais prieš juos įgyvendinant. 3.2. Tiekėjas turi turėti galimybę mokymus vykdyti nuotoliniu būdu.	**3. Requirements for the training session:** 3.1. After each major system change, the supplier undertakes to familiarize the buyer with the changes before they are implemented. 3.2. The Supplier must be able to provide a remote training.