Client's filing number of the Contract:	Contractor's contract registration number:
0227011249	

CONTRACT ON THE PROVISION OF SERVICES AND MODIFICATIONS FOR THE QUEUE MANAGEMENT AND PASSENGER FLOW MONITORING SYSTEM
(hereinafter the "**Contract**"):

Letiště Praha, a. s.

With its registered office at: Praha 6, K Letišti 1019/6, postal code: 161 00

incorporated in the Commercial Register administered by the Municipal Court in Prague, Section B, Entry 14003

Registration No.:   282 44 532

VAT No.:   CZ699003361

Bank details: Citibank Europe plc, organizational branch

Account number (EUR):   2052200409/2600, IBAN code: CZ03 2600 0000 0020 5220 0409

(hereinafter the "**Client**")

and

Xovis AG

with registered office at: Industriestrasse 1, 3052 Zollikofen, Switzerland

Incorporated in the Canton of Bern, Switzerland Commercial Register

Registration No.:   CHE-114.623.478

VAT No.:   CHE-114.623.478 MWST

Bank details: UBS Switzerland AG, Postfach, CH-8098 Zurich

account number (EUR):   IBAN: CH11 0023 0230 1962 9261X

(hereinafter the "**Contractor**")

The Client and the Contractor are hereinafter collectively referred to as "**Parties**" or individually as a "**Party**".

Preamble

Whereas:

(A)   The Contractor is interested in providing the Client with Services that are defined in this Contract,

(B)   the Client is the owner of the Hardware and the authorised user of the Software which together form the QMS,

(C)   The Contractor is a business company authorised to supply and modify the QMS and is interested in providing the Client with the Services specified below, as defined herein, and

(D)   the Client is interested in receiving Services related to the purchased QMS from the Contractor,

the Parties have agreed, in accordance with the applicable provisions of Act No. 89/2012 Coll., the Civil Code, as amended, as follows:

I. DEFINITIONS AND INTERPRETATIONS

I.1 The following expressions in this Contract have the meaning defined in this Art. **I.1**, it being understood that they are always capitalised in the text of the Contract:

I.1.1 "**Author's Work**" means any result of the Contractor's activity (other than Software-as-a-Service) created that becomes part of the Performance hereunder which shows the characteristics of work protected under the provisions of Section 2 of the Copyright Act.

I.1.2 The "**Copyright Act**" means Act No. 121/2000 Coll., on copyright, on rights related to copyright and on amendments to certain acts, as amended.

I.1.3 "**Customisation**" means setting the parameters of the Software according to the Client's needs and in accordance with the Client's instructions.

I.1.4 "Price for the Ordered Performance" means the Service Support Fee and/or the Price for the Ordered Performance pursuant to **Art. VII.1.2** hereof beyond the scope of the agreed service support.

I.1.5 The "**Man-Day**" means 8 (eight) hours of **work** by one Contractor's employee.

I.1.6 "**Work**" means to deliver and install the Hardware and make the Software available, including the necessary software equipment (if any) in the Place of Performance for the Client and to perform the installation, including assembly according to the schedule and in the location agreed on by the Client, and to transfer to the Client the ownership right to the delivered Hardware, to successfully perform the Installation and Integration of the Queue Management System and to provide the Client with non-exclusive Licenses/Sub-licenses for the proper use of the Software and to all Software outputs and Documentation, as per the Contract for Work number 0227011248.

I.1.7 "**Documentation**" means documentation describing the QMS and all its functionalities, properties and parameters, updated at each change to the queue management system, or after the handover of the relevant Ordered Performance.

I.1.8 "**Confidential Information**" has the meaning set forth in Art. **X.1** hereof.

I.1.9 "**Invoice**" means a tax document issued by the Contractor for the purpose of payment of the Price (i.e. Remuneration and/or Ordered Performance), whose requirements are set in **Art. VII.** hereof.

I.1.10 "**Error**" means (i) legal defects of the Ordered Performance, (ii) discrepancy between the actual properties of the QMS, Hardware of end devices and/or Software, and the properties set forth in the Documentation, or (iii) any deviation of the QMS, Hardware of end devices and/or Software from the standard properties described in the Documentation, which negatively affects its operation or functionality.

I.1.11 A "**Category A Error**" means the most serious Error manifested by the fact that:

(a) the QMS or any part thereof is completely non-functional or the Client cannot use the QMS or any part thereof, or

(b) the QMS does not meet the minimum requirements specified in the Functional and Technical Specification of the Queue Management System as set out in Annex 1 to this Contract for Work No. 0227011248 for each individual location installed,

To avoid any doubt, the Parties have agreed that a Category A Error will include an overall non-functionality of the Software and/or Hardware (of more than 50% of the measured area for each location and/or the QMS does not provide the required data or does not provide it in the required quality (accuracy), preventing the use of the QMS.

I.1.12 A "**Category B Error**" means an error manifested by the fact that the use or functionality of the QMS or any part thereof, or the functioning of the QMS, is limited by the Error, slowing down significantly the Client's processes, including sending measured data to other Client's systems.

To avoid any doubt, the Parties have agreed that a Category B Error includes a current non-functionality of the Software and/or Hardware on less than 50% but more than 10% of the measured area for each location unless it is a Category C Error.

I.1.1 A "**Category C Error**" means an Error which

(a) does not prevent or has minimum impact on the proper use or functionality of the QMS or any part thereof and/or of the QMS on the part of the Client, and

(b) has minimum impact on the Client's processes.

I.1.2 "**Hardware**" means the equipment (devices) forming part of the QMS as defined in Annex 1 to the Contract for Work, number 0227011248.

I.1.3 "**Implementation**" means the performance of all activities necessary to make the QMS operational, including but not limited to the installation and wiring of the Hardware in the Client's environment and making available the Software on the Client's hardware, including but not limited to the deployment of the Software and its components in the Client's environment and the integration of the Software into the Client's environment to ensure normal operation of the QMS.

I.1.4 The "**License**" means the right to access and use the Software or an Author's Work/Ordered Performance for the duration of the Contract.

I.1.5 The "**Time Limit for Response**" means the time limit within which the Contractor is obliged to inform the Client, by phone at **+420 2 2011 3000** (or another phone number designated for this purpose by the Client) and email at **servicedesk@prg.aero** (or another email address designated for this purpose by the Client), about the procedure to be taken to remove the reported Error or Unavailability and which employees of the Contractor will remove the reported Error or Unavailability.

I.1.6 The "**Time Limit for Removal**" means a time limit agreed to in this Contract in a binding manner, within which the Contractor is obliged to remove a reported Error or Unavailability.

I.1.7 "**Spare Parts**" means original spare parts and accessories such as end device hardware (sensors).

I.1.8 "**Unavailability**" or "**Unavailable**" means a condition when the QMS is not available as specified in the terms and conditions hereof.

I.1.9 "**Normal Operation**" means when the QMS operates and shows no Errors.

I.1.10 The "**Civil Code**" means Act No. **89/2012 Coll.**, the Civil Code, as amended, or a legal regulation replacing it in full or in part.

I.1.11 "**Remuneration**" has the meaning set forth in Art. **VII.1.1** hereof.

I.1.12 "**Verification Operation**" means the period of **fourteen (14) Calendar Days** from the Contractor's invitation during which actual data will be used to test the properties of the Software/Hardware, including the Ordered Performance, and the functionality according to the submitted Documentation, pursuant to Art. **IV.5**. hereof. For the avoidance of doubt, this is not a test of the whole QMS but only new the Ordered Performance.

I.1.13 "**Notification**" means a phone notification made by the Client to the Contractor's Support Centre concerning the existence of an Error or Unavailability. The Client will also confirm each telephone notification by sending an e-mail notification to the Contractor's e-mail address support@xovis.com by the end of the following working Day.

I.1.14 "**Continuous Information Period**" means the frequency of provision of regular information on the removal of Errors or Unavailability that the Contractor must provide to the Client.

I.1.15 "**Support Centre**" means the Contractor's Service Support Centre located (including staffing and technical support) at telephone number: +41 77 477 8426, e-mail address: support@xovis.com, URL address https://support.xovis.com .

I.1.16 "**Business Day**" means any calendar day except for Saturdays, Sundays, days off and non-working days within the meaning of the applicable legal regulations of the Czech Republic.

I.1.17 The "**Working Hours**" mean time from **9 AM to 5 PM CET** on Business Days.

I.1.18 "**Intellectual Property Rights**" means all patents, copyrights, rights to industrial designs, trademarks, trade names and business names, protected designations of origin, rights related to copyright, database rights, special rights of database makers, data models, rights in data, stored procedures, trade secrets, know-how and all other intellectual property rights of any nature (whether registered or unregistered), including any applications and exclusive rights to apply for protection of any of the above items anywhere in the world.

I.1.19 "**Handover**" means the day on which the Parties sign the Handover Report.

I.1.20 "**Handover Report**" means a handover and acceptance (paper or electronic) report of the Ordered Performance signed by both Parties.

I.1.21 "**QMS**" means the Hardware including Software designed to measure queue and passenger flows, also referred to "System" for accurate monitoring and analysis of passenger flows at key check-in points at the airport to enhance situational awareness of the handling process within the terminals, evaluate SLA performance and effectively plan the capacity of airport resources. The system is specified in the Contract for Work, number 0227011248 and in the Documentation.

I.1.22 "**Service Hours**" means **24 hours a day, 7 days a week, 365 days a year**.

I.1.23 "**Service Window**" means the time interval agreed to by the Client, during which the Contractor performs certain Software Corrections and/or service interventions that require a reduction of the System's operability or its total shutdown.

I.1.24 "**Services**" means the set of activities defined in **Art. III. and Art. IV.** hereof.

I.1.25 "**Software**" means a third party software applications and/or Software-as-a-Service application provided and/or made available by the Contractor to Client and specified in more detail in **Annex 1** to the Contract for Work, number 0227011248, forming part of the queue management and passenger flow measuring system designed to ensure the measurement of queues and passenger flows at selected locations at the airport and the visualisation of measured data in the user interface according to the parameters described in **Annex 1** to the Contract for Work, number 0227011248.

I.1.26 The "**Upgrade**" means the provision of new versions of the Software, particularly with an extended functionality, including the Implementation.

I.1.27 "**Update**" means the regular or irregular deployment of the Software updates or new Software versions, aiming to remove Errors or improve and enhance the Software, made by the Contractor.

I.1.28 The "**Modification**" has the meaning specified in Art. **IV.1.1** hereof.

I.1.29 "**Defect**" means (i) legal defects of the Ordered Performance or (ii) discrepancy between the actual properties of the Ordered Performance and the properties set forth for the Ordered Performance in this Contract or in the Documentation, or (iii) any deviation of the Ordered Performance from the standard properties described in the Contract or in the Documentation, which negatively affects its operation or functionality, providing that the Defect occurred before the Handover moment.

I.1.30 The "**Category A Defect**" means the most severe Defect manifested by the fact that:

(a) the delivered Ordered Performance has legal defects, or

(b) the Ordered Performance or any part thereof is completely non-functional or the Client cannot use the Ordered performance or any part thereof, or

(c) the Ordered Performance does not meet the minimum requirements specified in the Technical Specification of the Ordered performance pursuant to **Annex 4** hereto,

(d) the Ordered Performance causes non-functionality of the System or part thereof.

To avoid any doubt, the Parties have agreed that a Category A Defect will include an overall non-functionality of the Software and/or Hardware (of more than 50% of the measured area of the Ordered Performance and/or the Ordered Performance does not provide the required data or does not provide it in the required quality (accuracy), preventing the use of the Ordered Performance.

I.1.31 "**Category B Defect**" means a Defect manifested by the fact that the use or functionality of the Ordered Performance or any part thereof, or the functioning of the Ordered Performance, is limited by the Defect, slowing down significantly the Client's processes, including sending measured data to the Client's other systems.

To avoid any doubt, the Parties have agreed that a Category B Defect includes a current non-functionality of the Hardware on less than 50% but more than 10% of the measured area of the Ordered Performance unless it is a Category C Defect.

I.1.32 "**Category C Defect**" means a Defect which

(a) Does not prevent or has minimum impact on the proper use or functionality of the Ordered Performance or any part thereof and/or of the Ordered Performance on the part of the Client, and

(b) has minimum impact on the Client's processes.

I.2 Other expressions may be defined directly in the text of the Contract, with the definition of the expression being highlighted in bold and preceded by the words "**hereinafter**", and each time it occurs again later in the text of the Contract, it will be capitalised.

I.3 **Interpretation**

I.3.1 Words expressing only the singular include the plural and vice versa, words expressing the masculine gender include the feminine and neutral gender and vice versa, and words expressing persons include natural persons and legal entities and vice versa.

I.3.2 The headings of the articles and paragraphs of this Contract are provided for convenience only and will not be taken into account when interpreting this Contract.

I.3.3 In the event of any discrepancy between the text of this Contract and its Annexes, the text of this Contract will prevail.

II. SUBJECT MATTER OF THE CONTRACT

II.1 The subject-matter of this Contract is:

II.1.1 the Contractor's obligation to ensure the functionality of the QMS under the terms of Art. **III.1** of this Contract;

II.1.2 the Contractor's obligation to ensure support for the QMS within the scope of Art. **III.4** hereof;

II.1.3 the Contractor's obligation to provide the Client with framework modifications to the QMS (hereinafter the "**Modifications**") pursuant to Art. **IV.1** hereof.

and the Client's obligation to pay the Contractor for the performance that has been duly and timely provided the **Remuneration** according to Art. VII.1.1 of this Contract and the **Price for the Ordered Performance** determined in accordance with **Art. VII.1.2** of this Contract.

III. QMS FUNCTIONALITY AND SUPPORT

III.1 Functionality: During the Term of the Contract, the Contractor agrees to ensure the Normal Operation of the QMS pursuant to this Contract by removing Errors under the terms specified in this Contract.

III.2 During the Term of the Contract, the Contractor agrees to ensure that the QMS functions without any Errors.

III.3 Notification of Error. The Client is obliged to notify each Error or Unavailability to the Support Centre within such time after its detection that can be reasonably required from the Client.

III.4 Support Centre. The Contractor agrees to ensure during the Working Hours:

III.4.1 The availability of the Support Centre for making Notifications of Errors an Unavailability and for conducting telephone consultations with those Contractor's employees having appropriate qualifications (certification) and experience related to the QMS.

III.4.2 Maintaining records including the following information with respect to a notified Error or Unavailability:

(a) description of the course of action or conditions which led to the occurrence of the Error or Unavailability,

(b) at the Contractor's request, error statements,

(c) the Client's contact persons for dealings with the Contractor.

III.4.3 Responding to telephone or e-mail Notifications of Errors or Unavailability made to the Support Centre by the Contractor's responsible employees having appropriate qualifications (certification) and experience related to the QMS, while observing the Time Limits for Response under this Contract.

III.4.4 Providing telephone or e-mail consultations in relation to Errors and Unavailability;

III.4.5 The localising and identifying of Errors or Unavailability and their causes;

III.4.6 The provision of on-line information about the state, progress and manner of removing Errors or Unavailability during the the Continuous Information Period;

III.4.7 Updating the Documentation (if applicable) in the form of sending change reports so that the Client continuously has at its disposal up-to-date Documentation for the QMS that it is using at the given time.

III.4.8 Providing expert advice on the QMS and support in its use for the duration hereof. To exclude any doubts, the remuneration for the provision of professional consultations in the above extent are included in the Remuneration.

III.5 SLA. The Contractor agrees to observe the following time limits when providing Services:

Error Category or Unavailability (hereafter outage in this table)	Failure category description	Time Limit for Response time	Continuous Information Period	Time Limit for Removal
A	Complete QMS failure	1 hour	Every hour	12 hours if the failure cannot be solved remotely, in justified cases the presence of a service technician is required at Václav Havel Airport Prague within 24 hours
B	The use or functionality of the System or any part or operation of the System is limited by the Error	1 hour	Every hour	Within 24 hours, if the failure cannot be solved remotely, in justified cases the presence of a service technician is required at Václav Havel Airport Prague within 72 hours
C	Other problem or deficiency with minimal impact on QMS operation	24 hours	Every 24 hours	Within 14 calendar days, if the failure cannot be solved remotely, in justified cases the presence of a service technician is required at Václav Havel Airport Prague within 20 calendar days

III.5.1 The Time Limit for Response and the Time Limit for Removal referred to in this Article will start to run the moment the Notification was made by the Client to the Contractor's Support Centre. The same will apply for determining the Continuous Information Period.

III.5.2 The Parties agree on the procedure for providing continuous information as follows: the Client's employee contacts the Contractor's Support Centre within the agreed Continuous Information Period and the Contractor undertakes to inform the Client about the current status.

III.5.3 The Client is entitled to measure and test the QMS functionality using monitoring applications such as Nagios or SyDesk.

III.6 Removal of Errors of the QMS and Its Support.

III.6.1 The Contractor undertakes to remove Errors through Remote Access where practicable. If the Error cannot be removed through Remote Access of competent employees of the Contractor, the Client's employees can be invited by phone to cooperate in removing the Errors (hereinafter "**Telephone Support**"). Such an invitation to cooperate may only be made in the case of an Error where it is assumed that the time spent on removing the Error can be efficiently reduced in terms of eliminating the time needed for the Contractor's employees to appear at the Place of Performance.

III.6.2 In the case of the aforementioned cooperation of the Client's employees, the Contractor undertakes to proceed:

(i) with regard to the Client's employees' knowledge level of the QMS;

(ii) in cooperation with the Client's employee in a manner as if the Contractor was physically removing the Error, it being understood that the Contractor bears full responsibility for possible Errors and accidents caused by erroneous interference with the QMS.

III.6.3 The Parties declare that the aforementioned Telephone Support has no effect on the Notification and it is understood that the Error was reported to the Contractor and is removed by the Contractor.

III.6.4 If the Error cannot be removed through Remote Access or Telephone Support pursuant to **Art. III.6.1** hereof, the Contractor undertakes to come to the Place of Performance. In case of proven non-functionality of Remote Access due to the Client's fault, the time spent by the Contractor's technician on the way to the Client's Place of Performance will not be counted in the Time Limit for Removal of the Error. The Client is obliged to allow the Contractor access to the Place of Performance and to the QMS as required by the Contractor. Where the Time Limits for Removal of Errors specified in **Art. III.5** hereof are agreed in hours, the Client must allow Contractor access to the Place of Performance **24 (twenty-four) hours a day.** Where the Time Limits for Removal of Errors in **Art. III.5** hereof are agreed in Business Days, the Client is obliged to allow access to the Place of Performance during Working Hours.

III.7 Removal of Errors of the Hardware and its support.

III.7.1 While observing the Time Limit for Removal, the Contractor is entitled to remove the reported Error of the QMS and/or the Hardware in order to restore the Normal Operation only in any of the following ways:

(i) by replacing of the defective Hardware with new Hardware free from any defects, or

(ii) by repairing the Hardware, but only provided that a similar Error has not been subject matter of notification more than three times for the relevant Hardware, or

(iii) by agreement of the Parties on a manner of solving the removal of the Error other than as described in Art. **III.7.1(i)** or **III.7.1(ii)** hereof. The Parties will conclude a written agreement on another manner of removing the Error if it is agreed.

III.8 Removal of Errors of the Software and its support.

III.8.1 The Contractor undertakes to remove the Software Errors without undue delay by Installation of Software Corrections or by providing Updates and Upgrades of web application on an ongoing basis or in another manner so as to restore Normal Operation. Removal of reported Errors also includes removal of errors or faults occurred caused by the Error being removed or removal of errors in data which occurred due to the Error being removed.

III.8.2 The Contractor undertakes to inform the Client within **thirty (30) calendar days** from the issue of a new Update or Upgrade. Unless otherwise agreed between the Parties, the Contractor undertakes to perform Update or Upgrade of the Software released by the manufacturer of the Software during the Service Window. For the avoidance of all doubts, the Parties state that the provision of Update and Upgrade and all costs related form part of the Remuneration. The Contractor is further required (where it is reasonable) to submit an updated version of the Documentation to the Client within **thirty (30) calendar days** from the Update or Upgrade. Unless otherwise agreed by the Parties, the Update or Upgrade will not limit or remove the functionality of the QMS listed in Article 1 of **Annex 1 to the Contract for Work**, number 0227011248 or limit the functionality of the QMS.

III.8.3 Furthermore, the Contractor agrees to provide refresher training for Client's employee whose job duties include the operation of the QMS at the Client's request whenever major changes, QMS Upgrades or Updates.

III.9 Regular QMS maintenance

III.9.1 The subject matter of the Services is also performance of regular maintenance of the QMS at least once a year, consisting in:

(i) checking the overall functioning of the QMS,

(ii) performing Hardware maintenance if required for Normal Operation of the QMS.

III.9.2 After completing regular maintenance of the QMS, the Contractor is always obliged to prepare a written report on regular maintenance of the QMS, describing in detail all detected shortcomings and the course of action aiming at their removal.

III.10 Shutdown. Except for removal of a reported Error, the Contractor is entitled to shut the QMS down only during the Service Window. The Contractor must notify the Client of the Service Window at least **three (3) Business Day**s before its scheduled start. The parties have agreed that the total length of the Service Windows will not exceed **72 hours** (hereinafter the "**Scheduled Scope of Maintenance**"). A Service Window that is not notified to the Client at least **three (3) Business Days** before its scheduled start or that exceeds the Scheduled Scope of Maintenance is considered to represent Unavailability for the purposes of this Contract. The date of the service window must be agreed by both parties. For the avoidance of doubt, the Parties agree that the Contractor may deliver Updates as required without the need to shutdown the QMS.

III.11 QMS Functionality Guarantee. The Contractor undertakes that:

III.11.1 the sum of the total duration of Unavailability and the total duration of Category A Errors does not exceed **72 hours** per calendar year,

III.11.2 The total duration of Category B Errors will not exceed 480 **hours** per calendar year.

III.11.3 The total duration of Category C Errors will not exceed 90 calendar **days** per calendar year.

IV. MODIFICATIONS

IV.1 Assignment. During the term of the Contract, the Client is entitled to send to the Contractor, at any time, the assignment for

IV.1.1 make modifications and/or extensions and/or other changes to the QMS, including the delivery of Spare Parts and/or additional Hardware in accordance with the terms and conditions specified in **Annex 1 hereto**,

IV.1.2 provide expert advice in relation to the QMS,

IV.1.3 provide extraordinary training,

in the form of delivering the assignment by e-mail or in writing to the contact information of the Support Centre (hereinafter the "**Assignment**").

An extension under Art. IV.1.1 of the Contract may include the installation of a new QMS location, and a change under this Article may include the transfer of a QMS from a specific location to another.

IV.2 Offer. Unless the Client specifies a longer time limit, the Contractor undertakes to send to the Client's contact person specified in Art. XI.1.1 hereof, within **fifteen (15) Business Days** from the receipt of the Assignment, the price offer for the execution of the Assignment (hereinafter in this article the "**Offer**") which must include at least:

IV.2.1 the price for the implementation of the Assignment determined in accordance with Article VII hereof,

IV.2.2 requirements for cooperation and dependences by the Client,

IV.2.3 the estimated time schedule for the execution of the Assignment,

IV.2.4 the period of validity of the Offer which must not be shorter than **45 (forty-five) days**.

IV.3 Order. The Contractor undertakes to perform the Modification only on the basis of an order (hereinafter referred as **"Order"**) delivered to the contact information of the Support Centre.

IV.3.1 The following items will form an integral part and annex to the Client's Order:

(a) written specification of the extent of the Modification required by the Client and prepared with the wording corresponding to the Offer, and

(b) Offer.

IV.3.2 Within **fifteen (15) Business Days** from an Order's receipt, the Contractor agrees to accept the order and confirm its acceptance to the Client. If the Client does not receive a written rejection of the Order within the time limit according to the previous sentence, the Contractor is deemed to have accepted the Order.

IV.3.3 The Contractor is not obliged to accept and confirm to the Client the receipt of an order pursuant to Art. **IV.3.2** hereof providing that:

(a) the Client delivered to the Contractor an order for performance which is inconsistent with the Assignment or the Offer, or the terms and conditions of this Contract, or

(b) the Client failed to deliver an Order corresponding to the Offer to the Contractor within the period of validity of such Offer.

IV.3.4 For the avoidance of all doubts, the Parties have expressly agreed that an order received by the Contractor is an individual contract, the subject matter of which is the delivery of the performance specified in the individual contract (hereinafter the "**Ordered Performance**") for the price determined based on the Offer (hereinafter the "**Price for Ordered Performance**") and in accordance with the time schedule included in the Offer (hereinafter the „**Term of Delivery of Ordered Performance**"), and which will be governed by this Contract under all terms and conditions not expressly agreed to in the order (hereinafter the "**Partial Contract**"). Individual Orders will always refer to the filing number of this Contract in their text and will be numbered in ascending order.

IV.3.5 For the avoidance of doubt, the Parties have agreed that the Ordered Performance will always include if applicable and necessary an amendment to the Documentation containing updates of any changes associated with the Ordered Performance.

IV.4 Handover and Acceptance of Ordered Performance.

IV.4.1 The handover and acceptance of each Ordered Performance pursuant to Art. IV.1.1. hereof will take place on the basis of the acceptance procedure consisting of two phases:

(a) a Verification Operation, and

(b) the signing of a Handover Report.

IV.4.2 Where the subject matter of Ordered Performance is the provision of extraordinary training or services or expert consultations in relation to the QMS, the acceptance procedure will only include the signing of a Handover Report and no Verification Operation is required.

IV.5 Verification Operation.

IV.5.1 After the completion of the Ordered Performance, the Contractor will hand over the updated Documentation (if applicable) to the Client and invite the Client in writing to start the verification Operation. The time limit for launching the Verification Operation is **ten (10) Business Days** from the Contractor's invitation, unless otherwise agreed to by and between the Parties. If the Implementation is part of the Ordered Performance, the Contractor will carry out those activities no later than on the day preceding the day of commencement of the Verification Operation.

IV.5.2 If the Client fails to launch the Verification Operation and fails to do so even within an additional period of **five (5) Business Days** from the Contractor's repeated invitation, the Verification Operation will be deemed to be successfully passed without Defects.

IV.5.3 The Parties will write a record of the Verification Operation.

IV.5.4 If it is ascertained during the Verification Operation that the number of Defects does not exceed the following acceptance criteria:

(a) Category A Defects   0

(b) Category B Defects   0

(c) Category C Defects   3

the Contractor will be entitled to invite the Client to accept the Ordered Performance and the Client will be obliged to accept the Ordered Performance.

IV.5.5 If it results from the record of the performed Verification Operation that the Ordered Performance does not meet the acceptance criteria specified in Art. **IV.5.4** hereof, the Contractor undertakes to remove detected Defects no later than **ten (10) Business Days** from the result of the applicable Verification Operation and, after removing them, to invite the Client to commence the Verification Operation, Art. **IV.5** hereof being applied *mutatis mutandis*. This process of testing and subsequent removing of Defects will be repeated until the Contractor meets the acceptance criteria specified in Art. **IV.5.4**, but no more than twice.

IV.6   Handover Report.

IV.6.1 The Parties agree to sign a Handover Report after:

(a) The Parties make a record of a Verification Operation, and

(b) The Client checks and confirms the completeness of the updated Documentation.

IV.6.2 Each Handover Report will contain a list of remaining Defects with a time limit for their removal, it being understood that if such time limit is not agreed to in writing, it will be deemed to be **ten (10) Business Days** from the day on which the Handover Report was signed.

IV.7   Use of Ordered Performance.

IV.7.1 If the subject matter of Ordered Performance is

(a) the delivery of Hardware, the risk of damage to the Hardware will pass to the Client on the day of Handover and ownership rights and the on the day of full payment.

(b) the provision of a Software Licence and/or making the Software available, the Contractor, as the executor of the author's proprietary rights thereto will provide the Client with a non-exclusive Licence and/or right to use the Software on the date of delivery of the Ordered Performance of which such software is a part, namely

(i) for the period of duration of the Contract,

(ii) in the quantity necessary for using the Software in accordance with the Documentation and the Order,

(iii) granting a License to the Software, the Contractor grants the License to the Client as of the day of the Handover of the Ordered Performance which includes such Software, namely:

(iv) in the quantity necessary for using the Software in accordance with the Documentation and the Order and the terms of the Contract, and

(v) in compliance with the licensing terms specified in the Offer.

IV.7.2 By signing this Contract, the Client accepts the License and/or the Sub-license with effect as from the day of Handover of the relevant Ordered Performance. The remuneration for the granting of the License or the Sub-license forms part of the Price for the Ordered Performance.

IV.7.3 In connection with Author's Works created by the Contractor during the implementation of the Ordered Performance, especially in connection with the subject matter of the Modification, the Contractor will provide the Client with a territorially unlimited License for the duration of the Contractor's property rights as of the handover date of the Ordered Performance which includes the Author's Work, without limiting the scope and/or the manner of use and for the duration of the Author's property rights. The Client accepts the License. To avoid any doubt, the Parties state that

(a) the Contractor grants to the Client consent to use the Author's Work under the previous sentence either in its original or in an adapted or otherwise modified form, independently or as a set, or in connection with any other work or elements.

(b) the remuneration for the License under this Article is included in the Price for the Ordered Performance.

IV.7.4 If the licence terms and conditions of the Software enable so, the Contractor agrees that Author's Works created during the performance of the Ordered Performance, the Software, in respect of which the Client acquired the License and/or the Sub-license under this Contract in relation to the implementation of the Ordered Performance can be provided by the Client for use by the Authorised Persons, in any manner of use envisaged as of the date of signing the Contract by the Copyright Act and the Civil Code. The consideration for the use of the Software by the Client and the Controlled Entities is included in the Price for the Ordered Performance.

IV.8 To avoid any doubt, the Parties have agreed that making Modifications based on the Ordered Performance does not release the Contractor from liability for QMS Errors, except for temporary disagreements with the original version of the Documentation between the beginning of the implementation of the Ordered Performance and the Handover of the Ordered Performance. If the Client withdraws from the Partial Contract, the Contractor is required to restore the Software

into the state before the implementation of the Ordered Performance within **ten (10) Business Days** from the withdrawal.

IV.9 *Warranties.*

IV.9.1 The Contractor hereby assures the Client that, after the Ordered Performance is accepted by the Client and the remaining Defects detected during the acceptance of the Ordered Performance pursuant to Art. **IV.5.4** hereof are removed, the Ordered Performance will function in accordance with this Contract and the Documentation relating to the Ordered Performance.

IV.9.2 The Contractor hereby assures the Client that he will use the best practise methods and up to date tools to check and ensure that the Ordered Performance is free of any known viruses or malware that would prevent the Client from using the Ordered Performance or the System or that would cause that the Ordered Performance and/or the System stops functioning or that its functioning is limited or otherwise negatively impacted.

IV.9.3 The Contractor hereby provides the Client with a warranty that neither the Ordered Performance nor any other performance by the Contractor under this Contract nor the use of the Ordered Performance and/or the use of the QMS which includes the Ordered Performance by the Client under this Contract infringes or results in an infringement of any third-party Intellectual Property Rights. If the Contractor breaches its obligation resulting from the warranty mentioned in this paragraph, the Contractor will be responsible for all consequences resulting therefrom; it is particularly obliged to immediately secure for the Client the right to use the Ordered Performance and-/or the QMS including the Ordered Performance which does not infringe on any third-party Intellectual Property Rights and to compensate the Client for damage caused to the Client thereby, as well as for any non-material damage incurred by the Client.

IV.9.4 The warranty provided by the Contractor pursuant to Art. **IV.9.1** and/or Art. **IV.9.2** and/or Art. **IV.9.3** hereof will apply for the period of 24 (twenty-four) months from the day on which the Handover Report concerning the Ordered Performance or part thereof was signed. If any of the assurances pursuant to Art. **IV.9.1** and/or Art. **IV.9.2** and/or Art. **IV.9.3** hereof proves to be untrue during the period mentioned in the previous sentence, the Performance is deemed to have Errors. The Contractor undertakes to remove an Error of the Performance within **30 (thirty) Business Days** from the Client's Notification of the Error in the Place of Performance in one of the following manners:

(i)   by replacing the defective Hardware with new Hardware free from any defects, or

(ii)   by repairing the Hardware, but only provided that a similar Error has not been subject matter of notification more than three times for the relevant Hardware, or

(iii)   in cooperation with the Client using remote access or in person in the Place of Performance by removing the Error of the Ordered Performance which prevents proper use of the Ordered Performance, or

(iv)   by agreement of the Parties on a manner of solving the complaint other than those described in Art. (i), (ii) or (ii) hereof. The Parties will conclude a written agreement on another manner of removing the Error if it is agreed.

IV.9.5 In the event of replacement of the Hardware, the newly supplied Hardware must be delivered to the Place of Performance including the configuration (if requested by the Client when making the Notification).

IV.9.6 Disclaimer of liability for Errors. The Contractor will not be liable under the preceding provisions of this Art. **IV.9** hereof for an Error of the Ordered Performance, if it arises from the intervention of persons other than the Contractor or its subcontractors or due to Client using the Ordered Performance contrary to the Documentation handed over.

V. OTHER RIGHTS AND OBLIGATIONS OF THE PARTIES

V.1 Other rights of the Client. The Client is entitled to

V.1.1 to print and use the Documentation concerning the QMS in an unlimited number of copies, but only for the use of QMS by the Client and its business partners during the contract term,

V.1.2 participate in service interventions and to be present during the Installation, including operating tests of the entire QMS.

V.2 Cooperation Obligation. The Client undertakes to provide the Contractor with cooperation when carrying out Ordered Performance and service interventions in the case of Errors or QMS Unavailability; this cooperation consists in securing:

V.2.1 access to the Place of Performance,

V.2.2 the provision of information on the functioning of the QMS in the form of consultations with the Client's employees,

V.2.3 ensuring the operation of all technical (both software and hardware) infrastructure of the surrounding systems associated with the subject matter of this Contract,

V.2.4 securing conditions for Remote Access,

V.2.5 informing about Modifications in the QMS settings and Modifications of the Client's infrastructure having a direct influence on the functioning of the QMS.

V.3 A Failure to Cooperate. If the Client is in default with fulfilment of its obligations under this Contract, the Contractor undertakes to notify the Client in writing of this fact and to invite the Client to fulfil the relevant obligation within the additional period of **three (3) calendar days**. If the Client fails to fulfil its obligation even within the provided additional period of time, the Contractor will not be considered in default with its performance of any obligations relating to the Client's default.

V.4 Other Obligations of the Client. The Client agrees

V.4.1 to take care of the QMS with due diligence so that no damage is caused to the System and to prevent possible damage for occurring,

V.4.2 to promptly notify the Contractor, in a manner agreed to in this Contract, of any Errors or QMS Unavailability or the Ordered Performance or any claims made by third parties that prevent the Client from using the Ordered Performance, in the manner agreed upon herein,

V.4.3 to use the QMS, the Ordered Performance subject to regulations on the protection of Intellectual Property Rights in accordance with this Contract,

V.4.4 to use and secure all Documentation obtained as part of the use of the QMS so that no third party, except for the Client and its business partners, can obtain it without the Contractor's consent.

V.5 <u>Other Obligations of the Contractor</u>. Furthermore, the Contractor agrees:

V.5.1 to provide the Services using skill and care that can be expected from a competent communications and information technology services provider operating in the air transport industry, and through employees with sufficient education and experience in providing the given performance;

V.5.2 to adhere to generally binding regulations, technical standards and usual business practices relating to the Hardware and the Software.

V.5.3 to update the Documentation (if applicable and necessary) after each Modification and hand it over to the Client immediately after making the relevant Modification, but no later than twenty (20) Business Days from the written invitation by the Client. The Parties undertake to draw up a handover report on the handover and acceptance of the updated Documentation, which must be signed by both Parties.

V.5.4 to have all its liability for damage caused to the Client in connection with the performance under this Contract insured, at its own expense, with a solvent and reliable insurance company, in the extent usual for transactions of this type, but at least with an indemnity limit of **EUR 420,000 (four hundred and twenty thousand euros)**, and to maintain validity of this insurance for the entire term of the Contract. The Contractor undertakes to submit to the Client at its request a copy of the insurance contract within **ten (10) calendar days** at the latest. The Contractor is not entitled to reduce the amount of insurance coverage or to substantially change the terms and conditions of the insurance contracts under this Article with negative consequences for the Client without the Client's prior written consent,

V.5.5 to ensure that its workers or employees participating in the performance of this Contract adhere, when staying at the Place of Performance, to the internal regulations, instructions and directives, regulations governing the movement of persons, vehicles, material, fire safety, occupational health and other regulations with which they are acquainted by the Client, it being understood that a written report must be made of such acquainting,

V.5.6 to inform the Client about outstanding overdue receivables arisen on the basis of this Contract no later than **seven (7) Business Days** after the due date so that the Client may pay them without any delay,

V.5.7 to have a valid certificate throughout the entire term of this Contract, confirming that it is an authorised sales and service partner of the Manufacturer, and also to have, throughout the entire term of this Contract, at least **2 (two)** technicians certified by the Manufacturer for providing service support for the QMS (its employees or through a subcontractor). The Client is entitled to request that the Contractor submit such certificates at any time during

the term of this Contract and the Contractor will be obliged to submit the required certificates to the Client within **5 (five) Business Days.** If the Contractor does not submit copies of the certificates to the Client within the specified period of time, the Contractor undertakes to pay to the Client a contractual penalty in the amount of **0.1% from twelve times the amount of the Remuneration** for each day of default or part thereof. The payment of the contractual penalty will not affect the Client's right to be compensated for damage including non-material damage.

VI. LICENCE

VI.1   Pursuant to the Copyright Act, as amended, and the Civil Code, as amended, the Parties agree that the Contractor grants to the Client a Licence to use the Software created by the Contractor during the performance (if any) hereof, its Updates and Upgrades, the Ordered Performance and the Documentation and all other performance provided by the Contractor hereunder, which is subject to protection under the Copyright Act.

VI.2   Contractor grants Client a license to use the third party Software and/or Software developed by Contractor during the performance (if any) without any limitation for the duration of this Contract.

VI.3   Contractor grants Client a non-transferable and non-exclusive right to use existing (developed independently of this Contract) Software making available by the Contractor to the Client for the duration of this Contract.

VI.4   The Parties have agreed that the Client is not required to use the License.

VI.5   The Contractor agrees that the Client may use the QMS, including Updates and Upgrades, the Ordered Performance and the Documentation for its own benefit and for its own needs as well as for the benefit and for the needs of third parties – business partners. The Client is entitled to use the Software to such entities the Controlled Entities (a sub-licence).

VI.6   The consideration for the provision of the Licenses and/or rights to use pursuant to this **Art. VI** is included in the Remuneration pursuant to **Art. VII.1.1** hereof and/or the Price for the Ordered Performance pursuant to **Art. VII.1.2** hereof.

VII. PRICE, MATURITY, INVOICING

VII.1

VIII. TERM OF THE CONTRACT

VIII.1 This Contract comes into force on the date of signature by the last Party and becomes effective upon acceptance of phase 1 of the QMS installation pursuant to the Contract for Work, number 0227011248. However, if a special legal regulation stipulates that this Contract can take effect not earlier than on a certain day which comes later than the day on which this Contract was signed by the last Party, this Contract will take effect only on the earliest day on which the Contract can take effect pursuant to the special legal regulation. **This Contract is made for a definite period of time, namely for 5 years from its effective date.**

VIII.2 This Contract will cease to be valid and effective:

VIII.2.1 by written agreement of the Parties, or

VIII.2.2 after the expiration of the term for which it was made; or

VIII.2.3 by a termination notice given by the Contractor under Art. **VIII.3** where the notice period is **6 (six) months** and starts to run on the first day of the calendar month following the month in which the notice was delivered to the other Party; or

VIII.2.4 by a termination notice given by the Client without stating a reason or under Art. **VIII.4** hereof; the notice period is **three (3) months** and will start to run on the first day of the calendar month following the month in which the notice was delivered to the other Party.

VIII.2.5 by withdrawal from the Contract in cases specified in **Art. VIII.5** hereof.

VIII.3 The Contractor is entitled to terminate the Contract if

VIII.3.1 The Client is late with the payment of the Remuneration and/or the Price for the Ordered Performance for more than **30 (thirty) calendar days** from when it was due and will not pay the amount due even within an additional period of **14 (fourteen) calendar days** after the delivery of the Contractor's written request for payment.

VIII.4 The Client is entitled to terminate the Contract if:

VIII.4.1 The Contractor has repeatedly violated its obligations under this Contract, or

VIII.4.2 there is a breach of the warranties under Art. **IV.9** hereof where the Contractor fails to remedy the breach even within a period of time subsequently provided by the Client.

VIII.5 The manifestation of the will to withdraw from the Contract or from a Partial Contract must be made in writing and delivered to the other Party. The withdrawal will take effect upon the delivery of a notice of withdrawal to the other Party. Withdrawal from a Partial Contract will not affect the continuation of this Contract.

VIII.6 The Client and the Contractor have agreed that the Contract can only be terminated for those reasons expressly specified in this Contract unless mandatory provisions of applicable legal regulations provide the possibility to terminate the Contract for other reasons.

VIII.7 The Parties agree that even after the termination of the Contract in one of the manner specified in the Contract, the provisions on contractual penalties, including all contractual provisions that condition the right to a contractual penalties, damages, provisions related to Licenses, intellectual property rights ,confidential information, trade secret and the final provisions of the Contract will remain in force.

IX. CONTRACTUAL PENALTIES, LATE PAYMENT INTEREST, DAMAGES

IX.1 If the Contractor breaches its obligation to remove an Error or Unavailability within the Time Limit for Removal agreed to in **Art. III.5** hereof, the Client will be entitled to claim from the Contractor for each such breach a contractual penalty calculated on the basis of the following table:

Error category	Contractual Penalty
Category A Error or **Unavailability**	**0.3%** from the amount corresponding to a monthly Remuneration for each hour of delay
Category B Error	**0.2 %** from the amount corresponding to twelve times the monthly Remuneration for each day of default or part thereof
Category C Error	**0.1%** from the amount corresponding to twelve times the monthly Remuneration for each Working Day of default or part thereof

IX.2 If the Contractor breaches the guarantee for the Ordered Performance agreed to in Art. IV.9 hereof, the Client will be entitled to claim from the Contractor for each such breach a contractual penalty calculated on the basis of the following table:

Exceeding the allowed duration of Errors and/or Unavailability in a calendar year	Contractual Penalty
Unavailability + Category A Errors	**0.3%** of the amount corresponding to the monthly Remuneration for each hour exceeding the limit permitted pursuant to Article III.11.1 hereof
Category B Error	**0.2%** of the amount corresponding to twelve times the monthly Remuneration for each day exceeding the limit permitted pursuant to Article III.11.2 hereof
Category C Error	**0.1%** of the amount corresponding to twelve times the monthly Remuneration for each hour exceeding the limit permitted pursuant to Article III.11.3 hereof

IX.3 The Client has the right to demand from the Contractor:

IX.3.1 a contractual penalty in the amount of **EUR 410** for each case of breach of any obligation contained in **Art. III.4 a**nd/or **Art. III.6** to **III.10** and/or **Art. V.5** hereof, the Client is entitled to claim such contractual penalty from the Contractor even repeatedly if the state of breach of any of the obligations lasts for more than **2 (two) Business Days**, or

IX.3.2 a contractual fine in the amount of **EUR 210** for each case of breach of any of the obligations contained in **Art. IV.2** hereof, or

IX.3.3 a one-time contractual penalty in the amount of **EUR 410** and a contractual penalty in the amount of **0.1%** from the Price for the Ordered Performance for each day of default with proper fulfilment of the obligation where the Contractor breaches its obligation to remove Defects indicated in the Handover Report within **10 (ten) Business Days** from the signature of the Handover Report pursuant to Art. **IV.4** hereof and/or the obligation to **deliver the Ordered Performance according to the implementation schedule**.

IX.4 If the Contractor violates its obligation of confidentiality pursuant to **Art. X.2** hereof, it agrees to pay to the Client a contractual penalty in the amount of **EUR 20,410** for each individual case of infringement.

IX.5 If the Contractor breaches its obligation to process personal data pursuant to Art. **XII.2 to XII.4** hereof and/or the penalty provisions pursuant to **Art. XIII.4** hereof, the Contractor agrees to pay the Client a contractual penalty in the amount of **EUR 2,040** for each individual case of breach.

IX.6 If the Contractor breaches any obligation under **Annex 2** hereto, the Contractor agrees to pay to the Client a one-off contractual penalty amounting to **EUR 820** for each case of breach.

IX.7 If the Client fails to pay to the Contractor the Remuneration or the Price for the Ordered Performance within the maturity period agreed upon herein, the Contractor is entitled to claim from the Client a contractual late payment interest amounting to **0.02%** from the amount due for each day of default.

IX.8 The Contractor must pay the contractual penalty applied by the Client within **14 (fourteen) calendar days** from the date of written application of the contractual penalty by the Client, to the Client's bank account.

IX.9 The settlement of any contractual fine hereunder will be without prejudice to the Client's right to damages. If the Contractor causes any non-material damage to the Client, it is obliged to redress it.

IX.10 The Parties are not liable for any breach of their obligations under the Contract if such breach was due to circumstances that could not have been reasonably foreseen and /or is beyond the Party's control, which includes natural disasters, such as earthquakes, floods, storms, wars, and civil disturbances, pandemics, failure of third party service/hardware providers and networks. Employee strikes, administrative or judicial decisions issued against any Party are not regarded as circumstances ruling out liability. Notwithstanding any such obligation shall be limited to an amount equivalent to one and half times the Price with the exception of breaches of Confidential

Information and Intellectual Property which shall not be limited. For the purposes of this Art. the Price of the entire Work means the sum of Price of all phases of the Work in accordance with Contract for Work.

IX.11 A Party is obliged to inform the other Party about the nature of the obstacle that prevents it from performance of contractual obligations no later than on the second working day after it learned about the obstacle.

IX.12 The total penalties payable by the Contractor to the Client under this Contract shall not exceed in aggregate one and a half times the Price of this Contract. For the purposes of this Art. the Price of the entire Work means the sum of Price of all phases of the Work in accordance with Contract for Work.

X. PROTECTION OF INFORMATION

X.1 The Parties have agreed that all information disclosed by the Client and entered or sent to Software by the Client will remain confidential (hereinafter the "**Confidential Information**").

X.2 The Parties have agreed not disclose any Confidential Information to any third party and will take measures making it impossible for third parties to access such Confidential Information. The provisions of the previous sentence do not apply to cases where:

X.2.1 the Party's obligation herein is contrary to what is prescribed by law; and/or

X.2.2 such information to persons who are obliged by law to maintain confidentiality providing that the Party informs the other Party in writing to which third party the Confidential Information was made accessible and has bound this third party by the same confidentiality obligation by which the Party is bound; and/or

X.2.3 such information becomes publicly known or available in any manner other than by a breach of the obligations resulting from this Article; and/or

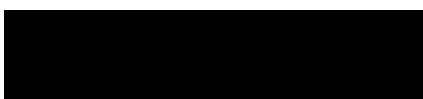X.2.4 the Party agrees in writing to making particular Confidential Information accessible.

XI. CONTACT DETAILS

XI.1 The Client's contact information

XI.1.1 for the purpose of sending Offers, Documentation and information on Updates and Upgrades:
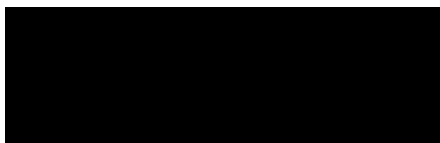
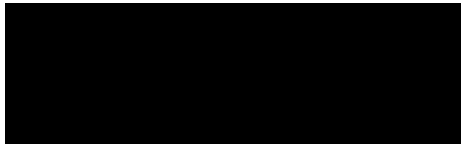XI.1.2 person authorised to sign the Order:

[REDACTED]

XI.1.3 Person authorised to act in contractual matters:
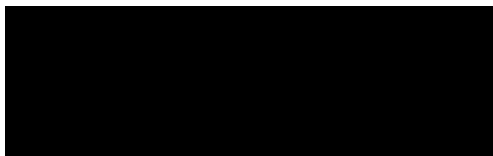
[REDACTED]

XI.2 The Contractor's contact information

XI.2.1 for the purpose of delivering Assignment and Orders:
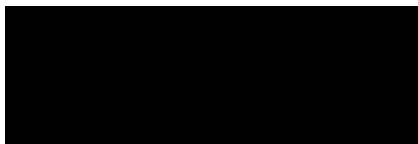
[REDACTED]

XI.2.2 for the purpose of other notifications and information under this Contract:

[REDACTED]

XI.3 Any notification or document which is to be delivered under this Contract, can be delivered in person or sent by registered post to the following address:

(a)   of the Client:
      Letiště Praha, a. s.
      K Letišti 6/1019, 160 08 Praha 6
      Czech Republic

(b)   of the Contractor:
      XOVIS AG
      Industriestrasse 1, 3052 Zollikofen, Switzerland

XI.4 The responsible representative to represent the Client in contractual matters related to the performance of this Contract is:

[REDACTED]

XI.5 The responsible representative to represent the Client in technical matters related to the performance of this Contract and in the matter of Errors, Defects, Assignment, Tenders and Orders **[REDACTED]**

[REDACTED]

XI.6 Client's contacts – authorised persons to represent the Client in technical matters

Name	E-mail	Telephone	Mobile
███████████████	████████████████████	█████████	█████████
███████████████	████████████████████	█████████	█████████

XI.7   Contact information in case of fire, leakage of an unknown substance or another emergency event:

Operations centre of the FB FP unit: 3333, 2222

Medical ambulance: 3301, 3302

Security control room: 1000

In case of any inquiries or suggestions for making improvements that are directed at individual areas:

    (i)   Occupational safety: bozp@prg.aero
    (ii)   Environment: zivotni.prostredi@prg.aero
    (iii)   Fire prevention: technik.po@prg.aero
    (iv)   Complaints: stiznosti@prg.aero

XI.8   Client's contacts – authorised persons in the matter of handling Errors, Defects and Modifications

Name	E-mail	Telephone	Mobile
██████	████████████████		
██████	████████████████████████████		
██████████	████████████████		

XI.9   Escalation contacts on the part of the Client:

Name	E-mail	Telephone	Mobile
█████████████	█████████████████████████		

XI.10 Escalation procedure on the part of the Contractor:

The Contractor's Support Centre with the contacts listed above is designated as a contact point to ensure a smooth handling of Errors. If the Client has doubts about the way of handling the problem, it is possible to use the following contact persons for escalation of the solution on the part of the Contractor:

Order	Contact	Person	Telephone	Cause of escalation
1.	████████████	█████████	█████████	████████
████████████				█████████
████████████				█████████
████████████		████████		

XI.11 Either Party is entitled to change its contact information by sending written notification to the other Party to the address specified in **Art. XI.3** hereof.

XII. DATA PROTECTION

XII.1 When performing this Contract, the Parties undertake to proceed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the "**Regulation**"), as well as in accordance with Act No. 110/2019 Coll., on the processing of personal data (hereinafter the "**PDP Act**").

XII.2 The Parties may process personal data solely for the purpose of performing this Contract. If the Contractor processes personal data for any other purposes, it does so contrary to the Contract, and the Client is not responsible for such processing of personal data. In this case, the Contractor is in the position of the personal data controller pursuant to the Regulation and the **PDP Act** in relation to these personal data.

XII.3 The Contractor undertakes to carry out the processing of personal data for the duration of the Contract and for a maximum period of **three (3)** months after its termination, after which it undertakes to destroy the data. If the Contractor processes personal data after the expiration of the period thus determined, it does so contrary to the Contract, and the Client is not responsible for such processing of personal data. In this case, the Contractor is in the position of the personal data controller pursuant to the Regulation and the **PDP Act** in relation to these personal data.

XII.4 Furthermore, the Contractor agrees to secure the processing of personal data using technical and organisational measures so that personal data are sufficiently protected and handled in accordance with the Regulation and the **PDP Act**. Personal data will be processed using computer technology and access to them must be sufficiently secured to prevent unauthorised or accidental access to personal data, their unauthorised modification, destruction or any other abuse or misuse.

XII.5 The Contractor undertakes not to combine personal data processed for the purpose of performing this Contract with any other personal data obtained or processed for any other reason.

XII.6 The Contractor is obliged to respect the data subject's right to the protection of their private and personal lives and to protection against unauthorised interference with the private and personal life of the data subject.

XIII. OTHER ARRANGEMENTS

XIII.1 The Contractor is not entitled to assign any of its rights under this Contract, even partially, to a third party without the Client's prior written consent.

XIII.2 The Parties have expressly and irrevocably agreed that:

XIII.2.1 The Contractor is entitled to set off its due and undue receivables from the Client only on the basis of a written agreement with the Client.

XIII.2.2 The Contractor is not entitled to pledge any of its receivables from the Client arising from this Contract.

XIII.3 Pursuant to Section 630 (2) of the Civil Code, the Parties have agreed to extend the limitation period in respect of the Client's rights resulting from this Contract to **10 (ten) years.**

XIII.4 By signing this Contract, the Contractor

XIII.4.1 represents and warrants that it is not an entity prohibited from trading in the Czech Republic by sanctions under Act No. 69/2006 Coll., on the Implementation of International Sanctions, as amended (hereinafter the "The Act on Sanctions"),

XIII.4.2 represents and warrants that it is not an entity which the public contracting authorities are obliged to exclude from procurement procedures pursuant to Act No. 134/2016 Coll., on Public Procurement, as amended (hereinafter the "PPA"),

XIII.4.3 represents and warrants that neither the Contractor, nor its beneficial owner is on the national sanctions list pursuant to Act No. 1/2023 Coll., on Restrictive Measures against Certain Serious Acts in International Relations (the Sanctions Act), as amended, or on a similar list of the European Union,

XIII.4.4 declares and warrants that any performance under this Contract will not be in violation of the Act on Sanctions or the PPA,

XIII.4.5 agrees to verify and ensure that all subcontracts that will form part of the performance under this Contract and all of Contractor's subcontractors that will participate in the performance of this Contract will comply with the terms of Art. XIII.4.1 to XIII.4.24 of this Contract.

XIII.5 Contractor's total aggregate liability to Client in respect of all actions, claims, losses, damages, costs and/or expenses arising out of or in connection with this Contract whether for breach of contract, in tort, under statute or any other law, is limited to an amount equal to one and a half times the Price. This Art. does not apply to damage caused intentionally or through gross negligence and in connection with the breach Confidential Information and Intellectual Property which shall not be limited. For the purposes of this Art. the Price of the entire Work means the sum of Price of all phases of the Work in accordance with Contract for Work.

XIV. FINAL PROVISIONS

XIV.1 If any of the provisions hereof is or becomes ineffective, and/or unenforceable, it will not affect the effect and enforceability of the remaining provisions of either the Annex or the Contract. The Parties hereby agree to replace any ineffective, or unenforceable provision with a new provision, the wording of which will correspond as close as possible to the wording of the original provision and the Contract as a whole.

XIV.2 This Contract together with the Contract for Work constitutes the entire agreement between the Parties concerning the subject matter of this Contract and replaces all other written or oral agreements made concerning the subject matter of this Contract.

XIV.3 If either Party fails to notice or waives any non-fulfilment, breach, default or failure to comply with any obligation under this Contract, such conduct will not constitute a waiver of such obligation with respect to its continued or subsequent non-fulfilment, breach or failure to comply, and no such waiver will be deemed effective unless it is expressed in writing in each individual case.

XIV.4 This Contract has been executed in t**wo (2) counterparts**, each having the force of an original. The Client will receive **one (1) counterpart** and the Contractor will receive **one (1) counterpart**. The Contract is made in the Czech language.

XIV.5 This Contract and the relations resulting from the Contract will be governed by the body of laws of the Czech Republic, particularly by the Civil Code.

XIV.6 The Contracting Parties have agreed that the provisions of Sections 1766, (change of circumstances), Section 1793 (disproportionate reduction), Section 1796 (usury), Section 1799, Section 1800 (contracts concluded as pre-formulated standard contracts), Section 2000 (cancellation of an obligation), Section 2050 (contractual fines and compensation for damages), Section 2093 (delivery of an excessive amount) and Section 2126 (self-help sales) of the Civil Code will not apply to this Contract or to the relationships resulting from the Contract. The Parties have expressly agreed on the following provisions of the Contract regulating their rights and obligations differently from the Civil Code:

XIV.6.1 The Contractor assumes, within the meaning of Section 1765(2) of the Civil Code, the risk of any substantial change in circumstances which may create a particularly gross disproportion in the rights and obligations of the Parties. The Contractor may not demand the renewal of negotiations on the Contract in the event of such substantial change in circumstances within the meaning of Section 1765(1) of the Civil Code.

XIV.6.2 Neither of the Parties is entitled to file any motions in court for a change of obligations under the Contract in accordance with the provision of Section 1766 of the Civil Code.

XIV.6.3 This Contract is concluded between entrepreneurs within the framework of their business; for this reason, the provisions of Sections 1793 to 1795 of the Civil Code on *laesio enormis* and the provisions of Section 1796 on usury will not apply to this Contract in accordance with Section 1797 of the Civil Code.

XIV.6.4 With regard to the conclusion of the Contract between entrepreneurs within the framework of their business, the Parties further agree in accordance with Section 1801 of the Civil Code that the provisions of Sections 1799 and 1800 of the Civil Code, on adhesion contracts, will not apply for the purpose of this Contract.

XIV.7 If one circumstance leads to a breach of multiple Articles of the Contract and, therefore, an obligation should rise on the part of the Client to pay a contractual penalty pursuant to two or more provisions of the Contract, the Contractor must pay to the Client a contractual penalty pursuant to that provision of the Contract which imposes an obligation to pay a higher contractual penalty.

XIV.8 The Parties have agreed that the provisions of Sections 1764 to 1766 of the Civil Code on changes to circumstances and the provisions of Sections 1793 to 1795 on disproportionate shortening will not apply to obligations arising from this Contract.

XIV.9 For the avoidance of any doubt, no obligation under this Contract is considered a fixed obligation pursuant to Section 1980 of the Civil Code.

XIV.10 Differently from Section 1987 (2) of the Civil Code, the Parties agree that a uncertain and/or indefinite claim by the Client is eligible for set-off.

XIV.11 No manifestation of the Parties' will made while negotiating or after entering into this Contract may be interpreted in conflict with the express provisions hereof, nor does it establish any obligation for either Party.

XIV.12 The Parties agree that they do not wish for any rights or obligations to be derived – beyond the express provisions of this Contract – from existing or future practices established between the Parties or any customary practices that are established generally or within the sector relating to the subject matter of this Contract, unless otherwise expressly agreed to in the Contract. In addition to the above, the Parties mutually confirm that they are not aware of any business customs or practices that have been established between them to date.

XIV.13 The Parties have mutually communicated all factual and legal circumstances which they knew or should have known as of the date of signature of this Contract and which are relevant in relation to the conclusion of this Contract. Apart from the assurances that the Parties have provided to each other in this Contract, neither Party will have any other rights or obligations in connection with any facts that become apparent and in respect of which the other Party did not provide information during negotiations on this Contract. One exception is those cases where the given Party intentionally and factually misled the other Party with regard to the subject matter of this Contract.

XIV.14 This Contract together with the Contract for Work contains the entire agreement concerning the subject matter of the Contract as well as all facts which the Parties should have or wanted to agree upon in the Contract and which they consider to be important in order to make this Contract binding. No manifestation of the Parties' intent made in negotiating this Contract or any manifestation of intent made after the execution of this Contract will be construed contrary to the express provisions of this Contract and will create any obligation on the part of either Party.

XIV.15 The Client notifies the Contractor and the Contractor acknowledges that the Client is a person referred to in Section 2(1)(m) of Act No. 340/2015 Coll., on Special Conditions of Effectiveness of Certain Contracts, Publication of Such Contracts and on the Register of Contracts (the Register of Contracts Act). This contract will be published in the Register of Contracts.

XIV.16 The Parties agree that all pricing-related information contained in this Contract, its annexes and Partial Contracts – including, without limitation, unit prices, discount structures, volume-based conditions, and payment terms - constitutes trade secrets within the meaning of Section 504 of the Civil Code. The Parties undertake to protect such trade secrets and to ensure their confidentiality, allowing access only to persons directly involved in the execution or performance of this Contract and only to the extent strictly necessary. For the avoidance of

doubts, the Parties declare that no other facts stated in this Contract, and its annexes, or Partial Contracts, apart from the pricing-related information specified above, shall be regarded as trade secrets unless expressly stated otherwise.

XIV.17 For the avoidance of doubts, the Parties agree that a bill of exchange cannot be used to satisfy pecuniary debt under this Contract.

XIV.18 The Parties expressly agree that general business terms and conditions or other similar terms and conditions of the Contractor will never apply to the relations regulated or foreseen by this Contract, not even if such terms and conditions form a part of the communication between the Parties.

XIV.19 The provisions of Sections 1932 and 1933 of the Civil Code will not apply to this Contract or liabilities under Partial Contracts. If there are multiple liabilities due that arise from this Contract, it is the Client's exclusive right to determine which liability will be paid first.

XIV.20 The Parties agree to resolve any and all disputes that may arise between them in connection with the performance or interpretation of this Contract through amicable negotiations and by mutual agreement. If the dispute in question cannot be resolved within **thirty (30) days** from the day on which it arose, such dispute will be submitted by either Party to a court with material and territorial jurisdiction. The Parties hereby agree that the court having the relevant territorial jurisdiction is the Client's general court pursuant to Section 89a of Act No. 99/1963 Coll., the Code of Civil Procedure, as amended.

XIV.21 This Contract may only be changed or amended by means of written, sequentially numbered amendments signed by both Parties.

XIV.22 Any and all annexes hereto form an integral part of the Contract and their list is as follows:

XIV.22.1 Annex 1: Price List of Spare Parts

XIV.22.2 Annex 2: Security Requirements

XIV.22.3 Annex 3: ICT Technical Standards

XIV.22.4 Annex 4: Functional and Technical Specification for Queue Management and Passenger Flow Monitoring

IN WITNESS WHEREOF the Parties have duly signed this Contract.

Date: 16.6.2025
On behalf of the Client:

Date:
On behalf of the Contractor:

Signature: _____
Name: Ing. Jiří Pos
Position: Chairman of the Board
Letiště Praha, a. s.

Signature: _____
Name: ██████████████
Position: ██████
Xovis AG

Signature: _____
Name: Ing. Martin Kučera MBA
Position: Member of the Board
Letiště Praha, a. s.

Signature _____
Name: ██████████████
Position: ████████
Xovis AG

Annex 1: Price List of Spare Parts
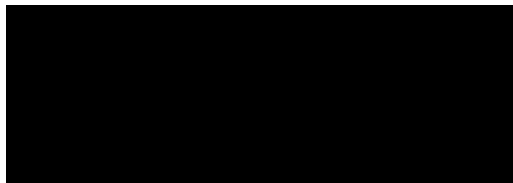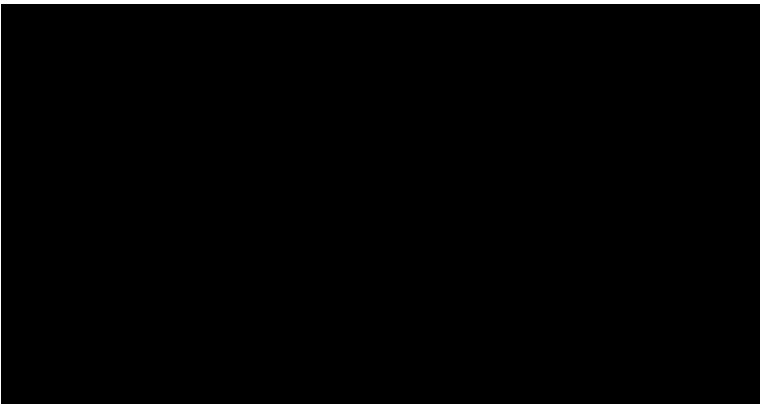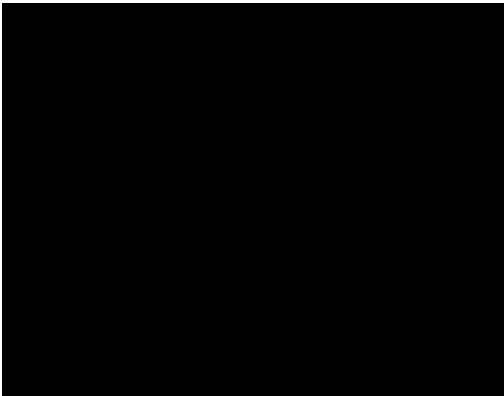
The Contractor can add other items as required, such as sensor parts, etc:

Annex 2 Security Requirements

1. **INTRODUCTION**

The purpose of this document is to define binding security, organisational and technical requirements for providers whose subject of performance for the Client is (exclusively or as part of the subject of performance of another service) the development, implementation and/or servicing of software or hardware (hereinafter also referred to as "SW" or "HW"), or who, in connection with the performance for the Client, access the Client's information system (hereinafter also referred to as "LP IS") and/or who, in the context of the performance for the Client, process and/or transmit and/or store and/or archive any data and information of the Client and/or its customers (hereinafter also the "Security Requirements").

2. **GENERAL REQUIREMENTS**

When providing performance to the Client, the Contractor agrees to meet the below obligations:

2.1. if the Contractor uses subcontractors in the provision of the performance, the Contractor undertakes to ensure compliance with the Safety Requirements also in contractual relations with its subcontractors, and the Contractor undertakes to prove this fact to the Client upon request by submitting the relevant contractual relationship concluded with this subcontractor, or by submitting an affidavit of proper fulfilment of this obligation;

2.2. Unless otherwise agreed by the Parties, the Contractor will appoint a responsible contact person for the purpose of ensuring compliance with the Security Requirements and related communication between the Parties (hereinafter also "**Contact Person**") within 3 days after the conclusion of the Contract.

2.3. Comply with the relevant provisions of the Client's safety policies, methodologies and procedures, respectively, the Client's applicable management documentation or parts thereof, if he/she has been acquainted with such documents or parts thereof.

2.4. within the time limit set by the Client, or without undue delay, to provide the Client with required cooperation to perform security testing of the provided Service;

2.5. Provide system and operational security documentation if modifications are made to the System that are not described in the existing documentation;

2.6. that if the performance also includes the installation of an operating system or third party SW, throughout its installation, only the latest updated versions of these products may be used;

2.7. Any and all information[1] obtained when providing the performance will not be stored unencrypted and will be protected against unauthorised access unless otherwise agreed to between the Parties in a particular case;

2.8. That the provided performance will include the installation of SW or its upgrade according to the hardening security policies and in accordance with the Client's security standards (this applies if the Contractor has been acquainted with the security standards);

2.9. That the ICT system will contain only compiled or executable code and other necessary data for operation of the ICT system;

2.10. That if the performance includes SW implementation in the LP's IS production environment, compliance of the software with the security requirements of hardening security policies must be checked before the launch of the software and if non-compliance is detected, compliance of the supplied software with the security requirements of hardening policies must be ensured without undue delay (this applies if the Contractor has been acquainted with the security standards).

2.11. The Contractor is responsible for ensuring that the sub-systems that are part of the Service contain tested, fully functional latest versions of security updates (patches)[2].

3. **PHYSICAL PROTECTION AND ENVIRONMENT SAFETY**

3.1. The Contractor undertakes to comply with the operating rules of the buildings (regime measures) and the premises used, especially in the area of physical protection of security zones where ICT system components or data carriers are located,

3.2. The Contractor undertakes not to leave freely available installation, backup or archive media or documentation for the ICT system, which is the subject of performance under this Contract, on the Workplace.

4. **Access Control**

If the performance includes access to external web services by LP employees, the following requirements must be met:

4.1.   The login data must not be stored in a readable form but must be protected by sufficiently strong cryptographic means.

4.2.   The system accessed by LP staff must be regularly tested, updated and sufficiently robust to ensure the security of information and data.

4.3.   In the event that the penetration testing results in critical findings, the Contractor will promptly inform LP of these facts and take sufficient and effective corrective action.

4.4.   The LP reserves the right to perform regular penetration testing throughout the term of the Contract.

4.5.   Access passwords must be sufficiently strong, i.e. at least 12 characters, password complexity (password must contain characters from at least 3 types), maximum and minimum password usage time and the possibility of password repetition must be adjustable.

If the performance includes access to the LP IS production environment, the following requirements must be met:

4.6.   The Contractor acknowledges that access to LP IS systems can only be granted to the physical identity of an employee of the Contractor or a subcontractor registered in the Client's identity register, based on the Contractor's request for access.

4.7.   Access passwords must be sufficiently strong, i.e. at least 12 characters, password complexity (password must contain characters from at least 3 types), maximum and minimum password usage time and the possibility of password repetition must be adjustable.

4.8.   The Contractor acknowledges that the Contractor's employee must demonstrably consent to the processing of personal data required for access, otherwise the Client is not obliged to grant access to the ICT system to the Contractor's employee. The Contractor's employee with assigned access (physical, logical) to the ICT system must demonstrably consent to the processing of personal data processed during the evaluation of data on movement and activities on the Client's premises (e.g.: monitoring using the Security Incident and Event Monitoring solution), where such consent must be given in writing or digitally by email, unless otherwise agreed by the Parties.

4.9.   The Contractor acknowledges that the authorisation provided to a Contractor's employee will be governed by the necessary minimum principle and is not claimable.

4.10.   The Contractor agrees that the access granted will not be shared by multiple employees of the Contractor or a subcontractor.

4.11.   The Contractor undertakes that access to the ICT system via the mobile app will only ever be via a secure VPN connection.

4.12.   The Contractor agrees that before connecting any end device, mobile end device or active network elements such as network switches, WiFi access points, routers or hubs to the computer network, the Contact Person on the Client's side will be asked for approval to make such connection.

4.13.   The Contractor undertakes to deactivate all unused network terminations and/or unused ports of the active network element without undue delay.

4.14.   The Contractor undertakes not to install and use these types of tools:
   - Keylogger,
   - Sniffer,
   - Vulnerability analyser and Port Scanner,
   - Backdoor, rootkit and trojan or other form of malware.

4.15.   The Contractor undertakes that all ICT systems of the Contractor that connect to the Client's network infrastructure are and will be protected against malware.

4.16.   The Contractor undertakes not to develop, compile or distribute any program code in any part of the ICT system that is intended to illegally control, disrupt or discredit the ICT system or illegally obtain data and information.

4.17.   The Contractor agrees to ensure that the persons involved in the performance provided to the Client:
   - not visit websites with ethically inappropriate content[3];
   - do not store and/or share ethically inappropriate content or information that is contrary to good morals or could damage the Client's reputation;
   - not download, share, store, archive and/or install data and executable files in violation of the License Terms or copyright law;
   - not store and/or share Company data and information on unauthorised data storage devices or media;
   - they weren't sending chain emails.

4.18. The Contractor undertakes to ensure that persons involved in the provision of performance to the Client who access the Client's internal network and/or ICT system respect and comply with the following restrictions. Laptop/computer type devices must have security patches applied (operating system, web browser and Java) and real-time anti-virus protection installed, running and updated;

4.19. The Contractor undertakes to ensure that persons involved in the provision of performance to the Client who access the Client's internal network and/or ICT system protect the authentication means and data to the Client's ICT systems. The Contractor acknowledges that in the event of unsuccessful attempts to authenticate the user, the relevant account may be blocked and dealt with as a security incident in accordance with the relevant management documentation and the relevant security incident management procedures may be applied (e.g. immediate revocation of access to the information assets of the natural persons of the external entity). The Contractor acknowledges that the procedure for handling a security incident or other consequence of a breach of the Security Requirements will not be considered as a circumstance excluding the Contractor's liability for delay in the proper and timely performance of the subject matter of the Contract and will not be the basis for any compensation for any damage to the Contractor or any other person on the part of the Client.

5. MONITORING

5.1. The Contractor acknowledges that all activities of the Contractor and their performance occurring in the Contracting Authority's system environment will be continuously and regularly monitored and evaluated by the Contracting Authority with respect to the content of the Contract and internal documents of the Contracting Authority with which the Contractor was acquainted.

5.2. The Contractor agrees to submit audit records containing monitoring results, successful and unsuccessful logins to the ICT system, and user management records to the Client upon request and without undue delay for the entire duration of the Contract, as well as after its termination for the period of 6 months.

6. DATA USAGE RIGHTS

6.1. The Contractor will be entitled to use the data submitted by the Client to the Contractor when providing performance for the Client, however, only to the extent necessary to fulfil the subject matter of the Contract.

6.2. The Contractor undertakes to handle the data only in accordance with the Contract and the relevant related legal regulations when providing performance for the Client.

7. INFORMATION EXCHANGE

7.1. If the subject of the Contract is the exchange of information between the Parties, the protection of such information must be ensured, in particular in the exchange, storage, archiving and termination of the Contract.

7.2. The Contractor undertakes that all transmission of data and information must be sufficiently secured in terms of the Client's security classification and therefore the requirements for confidentiality, integrity and availability of data and information.

7.3. The Contractor undertakes that online transactions carried out via web technologies will be protected by SSL certificates.

8. SECURITY INCIDENT MANAGEMENT

The Contractor undertakes, when providing performance for the Client, to ensure that in the event of an information security breach:

a. Immediately report the incident to the Client's Contact Person specified in the Contract;

b. in the event of a security incident and the subsequent management and evaluation of the security incident and/or in the event of a suspected security incident, provide the Client with the required cooperation (e.g.: provide logs and identification data (e.g. IP address, MAC address, HW type, serial number or IMEI) of the end device or mobile end device of the Contractor's employee or employee of the subcontractor involved in the performance, for content analysis, or implement the measures required by the Client without undue delay). Analyse the causes of the security incident and propose measures to prevent its recurrence if the Contractor caused or contributed to the security incident.

9. BUSINESS CONTINUITY MANAGEMENT

9.1. The Client is entitled to involve the Contractor in business continuity management, including the right to engage the Contractor in the business continuity plan related to IS LP and related services and/or include the Contractor in the Client's emergency plan.

9.2. The Client is obliged to inform the Contractor about the method of engagement in accordance with the previous paragraph.

9.3. The Contractor will submit to the Client the methodology of data backup and recovery in the form of a backup plan, test scenario of data recovery, record keeping system, and the system for ensuring the integrity and authenticity of the backup medium. The backup itself must be encrypted. As part of the delivery, the Contractor will also deliver and deploy the appropriate technological solution on which the data backup and recovery will be performed.

10. DATA DISPOSAL AND DESTRUCTION

10.1 If the Contractor is required to delete data and destroy technical media and/or operational data and/or information and copies thereof within the scope of the Contract, the Contractor will always comply with the data deletion rules so that the deleted data cannot be misused by unauthorised persons. The Client agrees to establish rules for the deletion of data and the disposal of technical media and/or operating data and/or information and copies thereof commensurate with the value and importance of the assets.

Annex 3: ICT Technical Standards

I.1 **Acronyms/abbreviations**

Acronym	Explanation
AS	Application server
LP	Letiště Praha, a. s.
DB	Database
DMZ	Demilitarised zone
FW	Firewall
ICT	Information and communication technologies – PA organisational unit
MQ	WebSphere MQ
OS	Operating System
D/INF	Director of OU ICT Infrastructure
ED/ICT	Executive Director of OU ICT
UNIX, WINDOWS, AIX, Linux, RedHat SUN, SYBASE, IBM, Oracle, etc.	Abbreviations of individual technologies by manufacturer and specialisation
TCP/IP	Network communication protocol
WMB	WebSphere Message Broker

I.2 **Terms**

Term	Explanation
Applications	Application/system providing required functionality for a specific group of users in PA
The Interface	Program element for connecting two or more different systems for data sharing or transmission
DMZ	Independent network separated by a FW. Access to computers and applications is controlled by FW rules
WebSphere MQ	Communication middleware for sending and receiving messages between distributed systems
Login	Unique username in the PA computer network environment
Worker	An employee of PA or any of its subsidiaries or an external employee (identified by their personal identification number)
User	An employee with access to the ICT environment (identified by their login)

II **Responsibilities and powers**

Name of the role / position	A description of responsibilities and powers

Administrator	A person providing application/system or technological layer administration (operating system, database, application server,…)
Application administrator	A person from the ICT department who is responsible for application operation, operational requirements (application shutdown, etc.) and change requirements (changes in functionality, modifications, application settings) for the application

III Binding technical standards for the ICT environment

The following standards are mandatory for all equipment and technology operated with in the internal environment of the PA computer network, regardless of the user.

(1) If any technology is operated in partial hosting mode (the entire technology is located within the premises of PA, but is separated from the internal environment by a firewall and is under the full management of the Contractor), an exemption from these standards may be granted.

(2) These standards do not apply to technologies operating in full hosting mode (the entire technology is located outside the internal environment of PA).

(3) Exceptions may always only be granted by the ED/ICT based on an agreement with other ICT components.

(4) Some technical standards are identified as critical. In these cases, in addition to an agreement, the ED/ICT himself/herself is required. These standards are indicated with an *

(5) Critical applications are all applications that require 24x7x365 operation/support, reliability above 99%, or a recovery time less than 30 minutes.

(6) If an application is placed within the Internet perimeter (it is displayed on the Internet) or forms a part of the backbone infrastructure, it is always considered critical.

(7) For applications located within the Internet perimeter, it will always be required to submit a positive penetration testing result performed by an independent entity (approved by PA) as part of the acceptance procedure. If the PA so requests, a revision of the application's source code may be required in the same way.

III.1 Servers

III.1.1 Operating systems

Application/system type	OS type*	Currently supported OS
Critical applications	(8) UNIX (9) Linux (10) (11) (12) Windows	(15) Linux (RedHat Enterprise 7.x and above) (16) Linux (Debian 9 distribution and above) (17) Linux (Ubuntu 18.04.1 LTS distribution and above) (18) Windows Server 2016 US and above (19) AIX 7.1 and above

	(13)			
	(14)	AIX		
(20) Other applications/systems (21) (22) (23) (24) (25)	(26) (27) (28) (29) (30) (31) (32)	UNIX Linux Windows AIX	(33) Linux (RedHat Enterprise 7.x and above) (34) Linux (Debian 9 distribution and above) (35) Linux (Ubuntu 18.04.1 LTS distribution and above) (36) (37) Windows Server 2016 US and above (38) (39) AIX 7.1 and above	

III.1.2

(40) Application/system type	(41) DB type*	(42) Currently supported versions
(43) Critical applications	(44) ORACLE (45) (46) (47) (48) SYBASE (49) (50) MS SQLServer (51) (52) MariaDB (53)	(54) 12.1 and higher – Enterprise Edition without any extra licensed option packs (Spatial, Partitioning) (55) (56) ASE – SYBASE 15 (57) (58) MS SQL Server 2017 and above (59) (60) 5.5 and above (61) 10.1. and above
Other applications/systems	(62) ORACLE (63) (64) (65) (66) MS SQLServer (67) (68) MariaDB	(69) 12.1 and higher – Enterprise Edition without any extra licensed option packs (Spatial, Partitioning) (70) (71) MS SQL Server 2017 and above (72) (73) 5.5 and above (74) 10.1. and above

III.1.3 Binding DB equipment setup

III.1.3.1 MS SQLServer

- The application database is primarily placed on a shared SQL Server for application databases. Only if the application cannot be placed on this shared server (due to performance, security, etc.), a separate SQL Server will be prepared for the application.
- The following rules apply to the shared MS SQL Server:
  - The Default Collation of the shared database server is "SQL_Latin1_General_CP1_CI_AS". The collation of the application database is set up as required by the application.
  - Applications/application accounts will have dbowner authority to the application database.
  - The application/application accounts will have no SQL Server administration level permission. (Sysadmin, Securityadmin, etc.)
  - Database roles are linked to ActiveDirectory groups
  - It is possible to use both SQL and Domain authentication for the application user.
    Only domain authentication can be used for user authentication.

III.1.3.2 ORACLE

- The database server is enrolled in the internal network perimeter DB and end-user direct access to this server is not allowed.

- Backup is performed using the RMAN utility

- The database name can only contain the characters A-Z and 0-9.

III.1.3.3 MariaDB

- Direct access to the database server is not permitted by end users

- The database name can only contain the characters a-z, A-Z and 0-9.

III.2 Communication

(1) TCP/IP v4, private address range under PA control (unless explicitly stated otherwise in PA requests).

(2) Topology and network elements are under the exclusive management of PA.

(3) The network environment is basically divided into 2 categories:

(3a) DMZ

- here are servers that can communicate directly with the Internet and provide certain services to Internet clients.

(3b) Internal

- here are servers and devices that are not allowed direct Internet access and are unavailable to Internet clients.

(4) Both environments will be protected by firewall gateways, and by default they cannot communicate with the Internet or to other DMZs or internal networks.

(5) Devices located in DMZs are not allowed to start communication with devices located within the internal environment. If it is necessary to publish some data on servers in the DMZ environment, it is necessary to upload it from the internal environment so that the transfer is started by the servers in the internal environment. Requirements for exemption from this rule are subject to prior approval of D/INF or ED/ICT.

(6) If DMZ servers are in a multi-tier architecture, all slave servers (application or database) must also be in the DMZ environment. This point respects the requirement regarding the prohibited establishment of communication from the DMZ to the internal environment.

(7) Users may only connect terminal devices to the data network and only in those places designated for them. It is strictly forbidden to connect devices such as routers, switches or wireless access points. Requirements for exemption from this rule are subject to prior approval of D/INF or ED/ICT.

III.3 B2B remote access

III.3.1 User remote access

(1) For remote access to the PA environment, the VPN Access Rules specify the standard operating procedure.

III.3.2 B2B remote access

(1) B2B remote access is intended for the permanent interconnection of the internal PA environment and the external company environment via an IPSec tunnel. This access is for application purposes only. This B2B remote access cannot be requested for remote administration purposes; User Remote Access is intended for these purposes.

(2) External companies with this access must guarantee that other parties have no access to systems in their environment using this interconnection, i.e. this is not a shared service.

(3) IPSec tunnel parameters are described in Annex 1.

(4) Implementation of B2B remote access is subject to prior approval of D/INF or ED/ICT.

III.4 Messaging Middleware

(1) Technology – BM Websphere Message Queue v 7.X *

(2) Data Layer – XML is primarily supported for exchanging data.

In case a different format is used, prior approval of ED/ICT is required.

III.5   Application servers

(1)   Currently operated:

Environment	AS type	Currently operated AS
UNIX environment	GlassFish	(75) GlassFish 3.x and above
Windows environment	(76) IIS	(77) IIS 10 and above

(2)   Application Windows Servers are regularly patched once a month using the WSUS service.

(3)   All application Windows Servers run the Forefront antivirus system.

(4)   An SCOM agent is installed on Windows Servers to monitor the server

(5)   An external balancer is used for GlassFish. HADB use is not supported.

(6)   To use AS from: WebSphere, Oracle AS or JBoss/Tomcat, prior approval of ED/ICT is required. Using AS outside this set is not allowed *

III.6 WWW applications

III.6.1 PA side

	WWW server *	Supported versions
All applications	Apache (78)	2.4. and above
	(79) MS IIS	IIS 10 and above
	(80) GlassFish	3.x and above*

(1) The specific version will be communicated by D/INF upon request. It is permitted to use PHP v. 7.0 or higher (in the internal environment – the specific version of supported SW is derived from the current versions in the official repositories of the OS being used).

(2) To use JAVA applets and ActiveX components, it is necessary to obtain prior approval of D/INF.

III.6.2 Client's side

(1)   Support for Google Chrome, MS Edge, MS IE 11.0 and higher is necessary *

III.7 E-mail, messaging

(1)   The internal mail system is based on the Microsoft Exchange platform, versions 2010 and 2013. Exchange Online Support – Office 365 support required

(2)   By default, EWS – Exchange Web Services is used for application access to the mailbox. Use of other protocols – IMAP, POP3 only with the approval of ED/ICT

(3) Sending e-mails within the application is possible only by using TLS and authentication by logging in with a domain user and password. Open Relay is not supported.

(4) Type B messaging is addressable via X400 and MQ.

(5) In order to use any cryptographic security, it is necessary to obtain prior approval of ED/ICT for the respective technology and the proposed process.

(6) PGP is the standard for cryptographic communication security.

III.8 Authentication

(1) All authentication rules are specified in the Identity and Access Management Directive.

(2) The base repository is Active Directory. To access LDAP, it is necessary to use a secure connection – use the LDAPS protocol.

III.9 Windows server infrastructure environment

III.9.1 Active directory

(1) Forest functional level and Domain functional Level of the CAH domain are set to "Windows Server 2016"

(2) Kerberos is primarily used for user authentication in ActiveDirectory. The use of LM and NTLM is prohibited. NTLMv2 can be used with the approval of ED/ICT. When using Basic authentication, it is necessary to use an encrypted connection.

(3) If a secure communication is used, the application must support TLS version 1.2 or higher

(4) The application must not require any permission in Active Directory beyond a routine user account in a routine operation

(5) MS ADFS services can be used to authenticate users in AD CAH

III.9.3 Application windows servers

(1) Applications must not require an interactive login to the server to run. This means that it must work in "service" mode, "scheduled task" mode, etc.

(2) The application account (local server or domain) must not be used for local login to the server. (Deny logon locally)

(3) Applications may not make entries in the Registry other than in the HKCU branch.

(4) If an application-database link exists, the application must not require installation on the same server as the database.

III.10 Terminal stations

III.10.1 Common terminal stations

(1) OS: Windows 10 Enterprise 32-bit and 64-bit

(2)   Office package: MS Office 2016, O365 CZ/US *

(3)   Users only have "User" rights

(4)   Computers are regularly patched using the WSUS service

(5)   Computers run the Forefont, Defender antivirus system

III.10.2 Limitations for applications/customers

(1)   Applications must not use "higher" permission than "User" to run

(2)   Applications must be compatible with the UAC security technology

(3)   Applications must support "silent installation"

(4)   Applications must run under Microsoft Application Virtualisation App-V

II.10.3 "Dumb" terminal stations

(1)   Operating System: Elux, EluxNG (Linux mutation)

(2)   Elux/EluxNG native clients: RDP, Citrix Metaframe, Mozilla, X11, XDCMP, VT320, ANSI terminal, 3250, 3270.

(3)   Dell Wyse P20

III.11 Terminal access

(1)   Microsoft Remote Desktop Services (RDS) platforms are supported.

(2)   RDP channel for peripherals (printers, COM ports, etc.) is not normally supported.

III.12 Virtualisation

(1)   VMWare is used for server virtualisation. Current version VMWare vSphere 5.5 or 6.5

(2)   When designing an application architecture, it is possible to use the VMware HA technology to ensure high availability of the virtual server. VMware SRM can be used to secure high availability of the application against DataCenter failure.

(3)   APP-V version 5 is used for end-to-end application virtualisation.

III.13 Development environment
The recommended development platforms are as follows:

III.13.1 Case for analytical work

(1) Enterprise Architect

(2) BPA

III.13.2 Source code management

(1) Subversion is used as the CVS repository

III.13.3 Terminal stations (PC)

(1) Delphi XE (if the application is developed internally or if the source code is passed to PA)

(2) C/C++

(3) C#

(4) JAVA 8

(5) .NET 4.0 Framework

(6) .NET 4.5 Framework and above

III.13.4 UNIX servers

(1) C, C++, JAVA

(2) JAVA 1.6. EE and above for applications working on the application server

(3) PHP v 5.3 and above

(4) Scripting languages - PERL, Shell, etc. - only after prior approval by ED/ICT.

III.13.5 NT Servers

(1) JAVA 8

(2) C/C++

(3) .NET 4.0 Framework

(4) .NET 4.5 Framework and above

(5) Visual WebGui

III.14 Individual IT environment standards for DMZ applications

The following standards apply to DMZ applications:

III.14.1 HW platform:
(1) Intel 64bit

III.14.2 **OS:**
(1) RedHat Enterprise Linux - x86_64 (release 6.x and above),

(2) Debian 8 and above,

(3) Ubuntu 12.04 and above,

III.14.3 **DB:**
(1) MySQL 5.1 and above (for non-sensitive data only)

(2) MariaDB 10.1 and above (for non-sensitive data only)

(3) Oracle 12.1 and above in ONE Standard Edition only

(4) MS SQL 2012 and above

III.14.4 **Application server**
(1) GlassFish Server 3.x and above

(2) Apache 2.4 and above

(3) Tomcat /JBoss

(4) IIS 10.0 and above

III.14.5 **Scripting languages**
(1) PHP 5.3 and above

(2) PERL 5.10 and above

(3) Shell – only with prior approval of ED/ICT

(4) The specific version will be communicated by D/INF upon request. The version of the supported SW will be derived from the current versions in official repositories of the OS used.

III.15 Cloud standards and applications running on It

(1) Devices located in the cloud are prohibited from communicating directly with devices located within the internal environment. If it is necessary to publish data from servers in the cloud to the internal environment, using an application interface, such as IBM MQ, Web Services is required

(2) The application interface must be located within the DMZ zone. Requirements for exemption from this rule are subject to prior approval of D/INF or ED/ICT.

III.16 Standards for using mobile devices to access applications

This access can be classified according to the environment from which they are gaining internal and external access.

III.16.1 Access from the internal environment

(1) If the devices are connected to the internal network, i.e. devices with MS Windows and included in the PA Active Directory, then all internal applications can be accessed.

III.16.2 Access from a trusted external environment

(1) A trusted external environment is private secure access such as 3G/4G access with a private APN operator or wireless network located on the airport premises secured by transmission channel authentication and encryption.

(2) Accesses to internal applications from this environment are subject to explicit approval by D/INF or ED/ICT after considering the risks arising from this.

III.16.3 Access from an untrusted external environment

(1) These include Internet access – e.g. 3G/4G connection, as well as access via the public wireless network on the airport premises. Devices connected to this environment can only access applications that are located in the DMZ and accessible from the Internet

47

III.17 Exceptions to these rules

(1) All exceptions to the above standards can only be applied with the express approval of ED/ICT.

IV   List of annexes

IV.1   Annex 1 – B2B IPSec Tunnel Parameters

Annex 1 – B2B IPSec Tunnel Parameters

Partner info		
Company:		*LP*
Address:		
City:		Prague
Country:		CZE
VPN endpoint		
Contractor:		Juniper
Type:		SRX 1400
Public IP Peer address:		
Mode	Main	
IKE Parameters – Phase 1		
Authentication Mode:	preshared key	
Preshared Key:	via sms	
Authentication Algorithm:	SHA2-256	
Encryption Algorithm:	AES-256-CBC	
Diffie-Hellman Group:	14	
Aggressive mode:	disabled	
Lifetime Measure:	time	
Lifetime (seconds):	28800	
IPSEC Parameters – Phase 2		
Protocol:	ESP	
Authentication Algorithm:	SHA2-256	
Encryption Algorithm:	AES-256-CBC	
Encapsulation Mode:	tunnel	
PFS:	No:	
PFS Group:	No:	
Lifetime Measure:	time	
Lifetime (seconds):	3600	
Local network		
Test IP for ICMP (ping)		
Technical Contact		
	e-mail:	e-mail:
	Telephone:	Telephone:
	comment:	comment:

Annex 4: Functional and Technical Specification for Queue Management and Passenger Flow Monitoring

1. **List of acronyms and terms:**

Acronym	Term	Explanation
QMS	Queue Monitoring System	Requested system for monitoring queues and passenger flows
API	Application Programming Interface	-
ATD	Actual Time of Departure	-
SCH	Security check	-
CAODB	Central Airport Operations Database	Commonly known as AODB
COB	Central check-point	The central security checkpoint in T2
EDW	Enterprise Data Warehouse	Data warehouse
EGG	Easy Go Gates	Automatic border control
FIDS	Flight Information Display System	-
GUI	Graphical User Interface	-
HK	Border control	-
ISH	Integration Service Hub	Data Integration Platform
KPI	Key Performance Indicator	The quantities measured or calculated by the system
LP	Letiště Praha, a. s.	Prague Airport Operator
MTBF	Mean Time between Failure	-
OS	Operating System	-
PAXMAN	Passenger Manager	Passenger Arrival Prediction System
PRINCE	Prague Airport Information Ecosystem	LP platform for sharing operational data and information between partners in the handling process
PRM	Passengers with reduced mobility	-
QM	Queue Management	Columns with stanchions for efficient queue management in front of the counters
SBD	Self-bag drop	Self-service baggage check-in counter
SLA	Service Level Agreement	-
STD	Scheduled Time of Departure	-
EU	European Union Nationality	Passengers of EU (and EEA) nationality passing through designated border control counters.
EU ABC	European Union Nationality – Automated Border Control	Travellers with EU (and EEA) nationality passing through automated border control e-gates.
All passports ABC	Third-Country Nationals - Automated Border Control	Passengers with EU (and EEA) nationality passing through automated border crossing points (e-gates).
All passports TCN EES	Third-Country Nationals – Entry-Exit System approved	Travellers of non-EU (and EEA) nationality who are already registered with EES, passing through designated border control counters.
All passports TCN nonEES	Third-Country Nationals – Entry-Exit System not approved	Passengers of non-EU (and EEA) nationality who are not registered with EES, passing through designated border control counters.

2. **Functional specification**

2.1 **General requirements**

2.1.1 Based on continuous monitoring of the premises at the specified locations, the system will monitor/calculate the quantities at the required accuracy and granularity defined in Annex 3_Minimum System Requirements in the second sheet entitled Minimum accuracy requirements. The economic operator will complete column F.

2.1.2 The System will provide dashboards with measured KPIs in real time and a refresh rate of less than 1 minute.

2.1.3 The System will capture and track at least 90% of all persons in a location at any given time, regardless of the number of persons found in that location.

2.1.4 The System will measure process times, collect data on passenger arrival times at individual checkpoints and counters, and collect data on passenger departures from counters and checkpoints.

2.1.5 The system must be able to distinguish between queues at two counters placed side by side in order to differentiate the measurement of process times, waiting times, etc., for different groups of passengers according to Art. 2.1.8.

2.1.6 The System will dynamically respond to changes in QM and the opening/closing of counters (see 2.1.7) or checkpoints and update the values of the measured quantities adequately and in a timely manner but no later than within 1 minute.

2.1.7 The system must be able to assess whether passengers at the border control counter (and EGG) or on the track at the security checkpoint are within a certain time interval (parameters to be set up according to the Client) and determine whether the counter or track is open/closed accordingly.

2.1.8 The System will differentiate between and evaluate queues, security check tracks and border control counters. This differentiation is necessary to allow for subsequent evaluation of the queues at:
a) security check: Economy/PRM and families/Fast Track/crew;
b) border control: EU/EU ABC/All passports ABC/ All passports TCN EES/ All passports TCN nonEES and Economy/Business (Fast Track)
c) any other processors that may arise in the future (health check, etc.)

2.1.9 The system will monitor and store the number of passengers currently waiting at the locations with the described subdivision on every minute.

2.1.10 The system will monitor and store the number of arriving passengers at these locations with the described subdivision, including the point in time when they arrived.

2.1.11 The system will monitor and store the number of passengers accessing counters at the locations with the described subdivision, including the time at which it occurred (individual passengers).

2.1.12 The system will monitor and store the number of passengers leaving the counters at these locations with the described subdivision, including the point in time when it occurred (individual passengers).

2.1.13 The system must generate alerts in the form of e-mails and text messages (see Sections 4.5.7 and 4.5.8) when events defined by the contracting authority or when definable levels (SLAs) are reached, such as exceeding the specified waiting time or an upward trend, exceeding the defined number of people in the area, etc. This setting must allow parametric changes by the contracting authority, separately in each monitored location.

2.1.14 The system will be capable of exchanging data with other systems (e.g. sending information on waiting times to CAODB or other systems in real time via the interfaces described in Section 4.

2.1.15 The system must allow SLA parameters to be changed on a specific date while preserving the history of previous parameters.

2.1.16 The system will store the history of all measured data including the possibility of displaying them in GUI according to entered parameters for up to 2 previous IATA seasons.

2.1.17 The Live View dashboard must provide a visual overview of the current situation including all available KPIs in all monitored locations.

2.1.18 The system must be able to predict the waiting time.

2.2 Data visualisation

2.2.1 Visualisation and access to data via a real-time web interface in an intuitive and user-friendly form. Individual reports on the current situation at the process points can be set or adjusted by the user or according to the assigned role.

2.2.2 The queue measurement system will be able to display data in a dashboard according to the following requirements:

- Primary visualisation summarising the current situation in all measured locations with defined KPIs and alarms of current SLA performance (performance limits will be set by the Client)

- A detailed overview of the selected location with information on the current waiting time (overall and by queue), the number of passengers, the number of open process points, and the predicted waiting time.

- Live View visualisation – the ability to select a location and see the current status online = display of all persons (anonymised) and queues in a given area (the data must be displayed with a maximum delay of 15 seconds compared to real time). In their tender, each economic operator can attach a visualisation rendering from its system. In addition, data must be displayed according to the following parameters:
  - o the current waiting time
  - o the number of persons waiting in an area/queue;
  - o the number of active gates/counters at a checkpoint;
  - o the predicted waiting time with respect to the current number of open filters (counters, tracks, etc.)

2.2.3 The possibility to select current data or data history by time period at least within 2 previous full IATA seasons (possibility to select days, hours, minutes) and also possibility to filter data by:

- individual checkpoints at security and border control;
- monitored checkpoints (border control, security check)
- an overview of SLA violations at security and border control checkpoints over a specific period of time;
- throughput (process times) for individual lines for security and border control; process times must also be stored in the detail of individual passes (individuals) for each of the counters/lines
- the possibility to view the history of individual process points with an overview of passengers and process times.

2.2.4 The system will allow the administrator to access system configuration and status information about the system and its components.

2.2.5 The system must allow the Contracting Authority to define reports that will be generated and sent to e-mail addresses designated by the Contracting Authority in a selected format on a regular basis.

2.3 Minimum accuracy requirements

The following table defines the minimum accuracy requirements for System measurements. The economic operator will fill in this table according to the parameters of its own system in Annex 3_Minimum System Requirements for the system in the second sheet entitled Minimum Accuracy Requirements.

Parameter	Accuracy
Counting of persons ***The number of persons crossing a defined virtual border from both directions***	>95% *The max. error of the sum of persons who cross the defined line must be less than 5%.*
Actual waiting time [min] ***Actual passenger waiting time***	>85% *The maximum error in measuring the actual waiting time of a particular passenger must be less than 15%.*
Predicted waiting time [min] ***The predicted waiting time of a passenger who enters the queue last***	>80% *The accuracy of the predicted waiting time must be higher than 80%, i.e. for an actual waiting time of 10 minutes, the error can be 2 minutes at most.*
The number of persons arriving in a queue ***The number of persons arriving in the queue***	>95% *The number of captured incoming persons must be higher than 95%.*
Throughput [PAX/h] ***Current passenger clearance rate at a specific checkpoint (e.g. security line) or check-in point (a complete security checkpoint)***	>90% *The number of passengers registered must be greater than 90% of all passengers passing through the check-in point.*
Process time [s] ***The duration of a specific process (check-in, security checks, etc.) for the passenger***	>90% *The maximum error in measuring the process time for a particular passenger must be less than 10%.*

## 3. Specification of monitoring locations

3.1 Terminal 1

Departure Border Control

The departure border control is located in Terminal 1 for flights departing to outside the Schengen area. 100 percent of passengers departing from T1 pass through this process point. Passenger flow is divided into passengers from EU countries (and some others) and other countries. EU passengers have the option to use the automatic border control in the form of Easygates (Area F) but to do that, they must have a biometric passport and be older than 15 years. EU passengers who do not meet this requirement can use the EU counters (Area E) or the All Passports counters (D), designated primarily for passengers from other countries. A special group of passengers are passengers who meet the conditions for Fast Track, passengers with reduced mobility (PRM), families with children and CREW/airline crew (Area G).

Entry to the border control area is recorded with boarding pass validators. The division of passenger flows is as follows: All passports (A), EU passports (B) and Fast Track and PRM (C).

Dimensions
- Area behind the validators: 383.9 square metres
- Ceiling height: 3.25 m
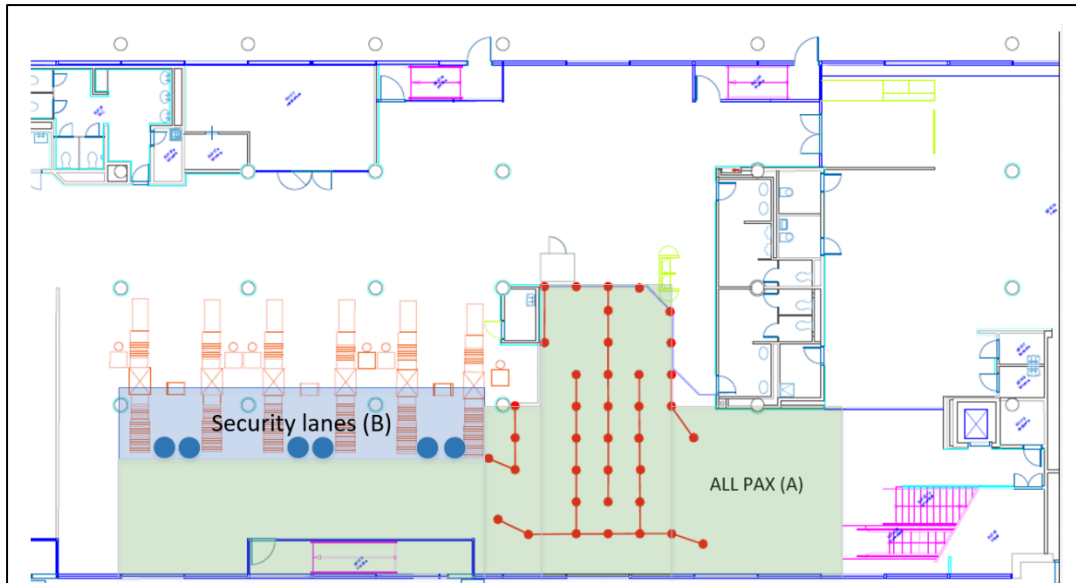
Centralised security check in pier B

On the ground floor of Terminal 1, pier B, which serves flights to other non-Schengen countries, there is a centralised security checkpoint for bus gates B10 to B18. Monitoring will be carried out in two areas, Area A (QM) and Area B (security check area after X-ray).

Dimensions
- Areas A+B
  - Area size: 450 m^2
  - Ceiling height: 3.3 m
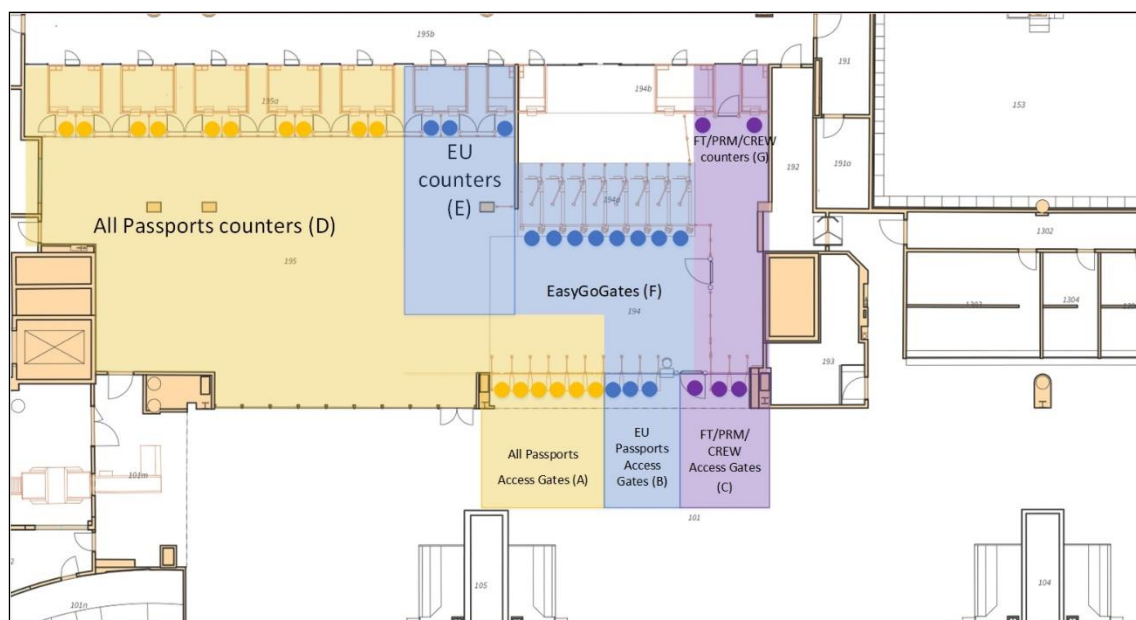
Arrival

Border Control

Arrivals border control is located in Terminal 1 for arrivals from outside the Schengen area. Passengers arriving from these countries who do not pass through the transit area in order to depart from Terminal 2 pass through this process point.

Passenger flows are divided before the border control point itself as follows:
- passengers who are authorised to use automatic border control via Easygogates in Area A (EU i TCN),
- EU passengers who have the option of using dedicated counters in Area B, and

- Passengers with Fast track check-in authorisation who are primarily handled in Area C.
- The other counters are for all passengers (area D) – with a division between those already registered in the EES system and others.
- In addition to monitoring the border control area, the LP aims to monitor the corridors leading to this checkpoint, namely the corridors from piers A and B.
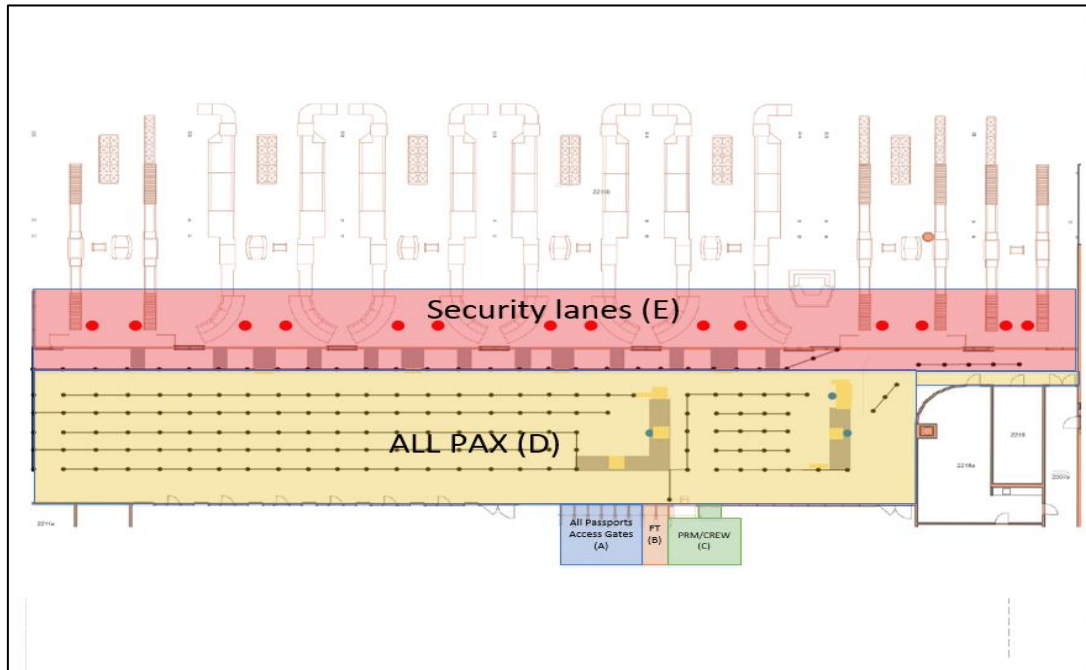
Dimensions
- Area size:
  - A = 77 m^2
  - B = 108 m^2
  - C = 82 m^2
  - D = 492 m^2
  - Ceiling height (A-D): 2.5 – 3.5 m
  - E = 848 m^2
    - Ceiling height = 3.9 m
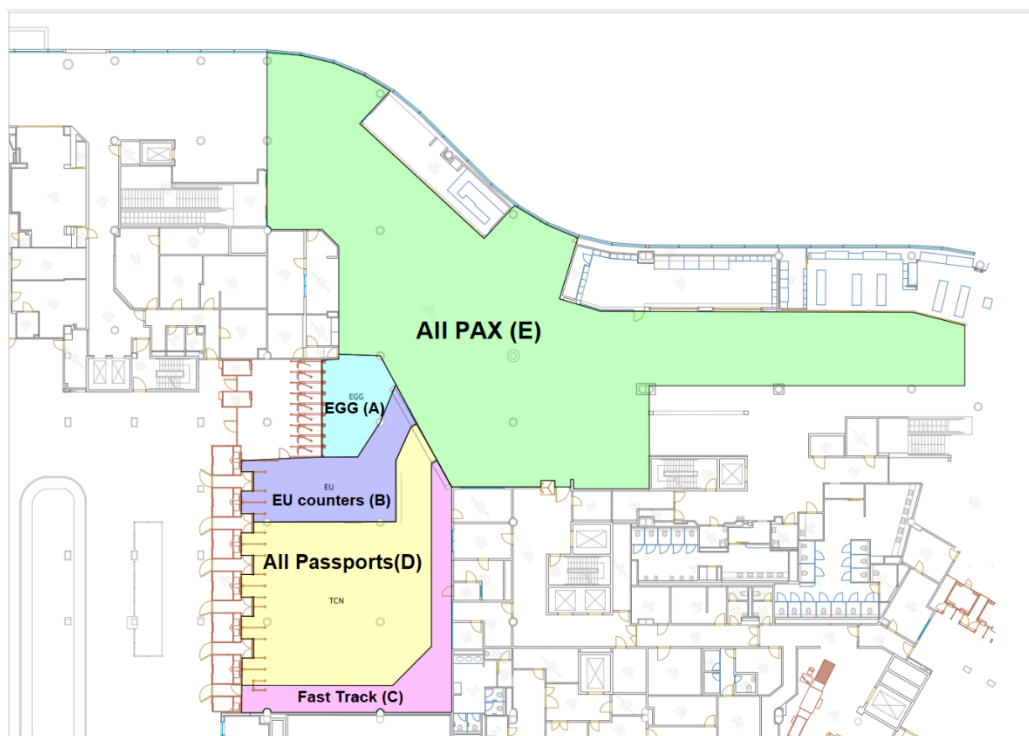
- **3.2   Terminal 2**

Central Security Control (COB)

The central security control, consisting of 14 security lines, is located in the south-east of the Terminal 2 departure hall. The monitored area consists of three areas. The area in front of the boarding pass validators is further subdivided by passenger group into Area A for all passengers, Area B reserved for Fast Track passengers, and Area C for PRM passengers, CREW and families. This is followed by Area D, where passengers undergo QM, and finally the security check area itself where passengers and their hand luggage are screened (Area E).

Dimensions

- Areas A + B + C
    - Area size = 90 square metres
    - Ceiling height = 18.8 m
- Area D
    - Area size = 733.8 square metres
    - Ceiling height = 18 m
- Area E
    - Area size = 1240 square metres
    - Ceiling height = 5 m

3.3   System installation plan

The installation of hardware and commissioning of the queuing system is expected to take place on a site-by-site basis according to the following plan. The Client reserves the right to modify the proposed phasing.

Phase 1: Centralised security checkpoint in pier B (T1)

Phase 2: Departure passport control (T1)

Phase 3: Arrival passport control (T1)

Phase 4: Centralised security checkpoint (T2)

4.   Technical specifications

4.1   Description of existing infrastructure

4.1.1   Boarding Pass Validators

Boarding pass validators or automatic Kaba gates are installed at LP to control access to the airside area. Eleven of them are re located at Terminal 1 in front of border control and eight of them at Terminal 2 in front of COB. The gates validate access authorisation by reading a barcode from a particular passenger's boarding pass. This information is then recorded in the AirSphere PaxControl system which is used to control and administer the gates. This data is available for possible matching with other available data. However, as far as the use of personal data is concerned, the restrictions imposed by the GDPR must be taken into account.

4.1.2   CAODB

A central operational database, commonly known as AODB.

CAODB receives and integrates data for individual flights at PRG airport and then provides this integrated data to other systems (ATC, RMS, ARES, AFA, SCORE, ASMGCS, handling companies, airline carriers, etc.).

CAODB offers a user interface for PRINCE control rooms and xMAN modules that provide operators with the necessary information and tools for operational management of the aircraft check-in process.

4.1.3   ISH

ISH is an event-based system built on the Kafka messaging platform capable of providing two-way data exchange between the System and other producers or consumers of data exchange.

4.2   General requirements

4.2.1   In general, the delivered solution must be easily expandable, configurable and scalable in terms of HW and SW according to LP requirements for changes in operation, scaling up or further development of LP.

4.2.2   As part of their tender, each economic operator must include a detailed design of the system architecture, including communication links of all proposed components (network protocols and ports). All communication within the system will be secure and, if web interfaces are used, encrypted and secured with a certificate.

4.2.3   The economic operator must propose the number of monitoring devices at each of the locations described herein. The economic operator will also provide a detailed plan for the installation and placement of sensors based on physical capabilities and inspections of the LP premises. The actual installation of the sensors will be carried out by the Contractor. If it is necessary to install the sensors up to the level of the roof structure as part of the installation at the Centralised Security Check (T2) location, the Contractor will, in addition to the installation itself, run the necessary structured cabling from the connection point (data switchboard) located on the walkway below the roof level of Terminal 2 to the individual sensors.

4.2.4   The monitoring equipment will be robust with a MTBF of at least 10 years and changes in illumination, artificial and natural light or shadows will not affect the accuracy of the monitoring.

4.2.5   The monitoring equipment will be capable of being installed and operated at ceiling heights ranging from 2,5 m to 20 m.

4.2.6   Queue management equipment must not interfere with security cameras or other airport systems without compromising security and their functionality.

4.2.7   The queue management equipment must not in any way interfere with or restrict the work of the state security forces (The Police of the Czech Republic, The Customs Administration of the Czech Republic).

4.2.8   The System will be able to completely cover larger areas by overlaying a number of monitoring devices and will accurately track persons in the area with a positional accuracy of 30 cm and assign a unique ID to each person.

4.2.9   The System will provide the following components:
- Dashboards
- A reporting module
- Notifications via e-mail and text messages
- Standard API
- The management of monitoring devices
- System management and monitoring

4.2.10   The tender will include the cost of supplying and installing the monitoring equipment.

4.2.11   The economic operator will provide the minimum network connectivity requirements for the system.

4.2.12   The System will be fully developed and offer a stable and accurate operation from the moment of launch. No major developments need to be made to meet the requirements described in this document.

4.2.13   The System will be able to create/generate and export reports in .xls, .csv and .pdf format within its GUI.

4.3   Server

4.3.1   A cloud solution provided by the Contractor is required.

4.3.2   All system events will be logged and stored for diagnostic and auditing purposes.

4.4   Application

4.4.1   All functions of the Queue Measuring System will be accessible via a single Graphical User Interface (GUI), either as an installed desktop application or a web-based interface. Access via a web interface will be secured with a certificate (an https protocol).

4.4.2   The application will be adapted for Microsoft Windows 10 and 11 64bit.

4.4.3   In the case of a web application, the System will support display via a standard web browser, preferably without the need for any other commercial software component, and will support the latest version of at least one of the following web browsers: MS Edge, Google Chrome.

4.4.4   The System will also support access to the web interface or the application via a mobile device such as a tablet or mobile telephone regardless of the OS. This means the display must be responsive.

4.4.5   The System will support the transfer of data and alerts to other airport systems such as the Data Warehouse (EDW), inPAXMAN, PAXMAN, PRINCE, FIDS or similar systems used by LP, for more details see Art. 4.5.

4.4.6   The Queue Measurement System application will allow simultaneous access by as many as 100 users.

4.4.7   User authentication will preferably be handled by Oauth 2.0 and JSON Web Tokens using Azure Active Directory of the Contracting Authority. If this is not possible, access will be addressed at the application level.

4.4.8.   User access to the System via SSO is preferred or will be conditional on the user entering a username and password. If application logins are used, the System will allow setting requirements for user passwords, such as minimum password length and mandatory use of different types of characters, and will also allow setting the maximum password validity period and the possibility of password repetition.

4.4.8   The Queue Measurement System will allow for the definition and setting of user roles and the assignment of these roles to specific users. At a minimum, the following roles will exist in the System with the following permissions:

- Users:
  a) Permission to access the system (login)
  b) Possibility to change the password (for application accounts)
  c) Report generation and data export
  d) Ability to access and use system functions based on user rights and permissions set by the administrator

- Administrator:
  a) Administrative work with the system
  b) Possibility to customise system parameters according to user needs
  c) Ability to set rules and data for specific users/groups of users
  d) Manage access permissions for individual users and roles

4.4.9   The Queue Measurement System must also enable LP to set a maximum number of failed authentications or password entries. Once this value has been exceeded, the login account will be disabled and can only be reactivated by the system administrator.

4.4.10   All user or administrator modifications made to configuration and settings, including editing of user accounts or roles, will be logged and these logs will be retained in the system for at least 12 months.

4.5   Interface

4.5.1   The System will allow real-time data exchange (export/import) with other systems via the Integration Service Hub (ISH) and batch data export to the LP data warehouse.

4.5.2   The Queue Measurement System will be capable of sending minimally the following data in real time to the ISH and subsequently to the CAODB:

- Up-to-date data on actual waiting times (including predicted ones) at selected locations, for presentation to passengers through various communication channels (FIDS screens, websites, mobile applications, operational applications such as PAXMAN, etc.);

4.5.3   The following data can be sent from CAODB via ISH to the Queue Measurement System:
- Data on opening/closing times of border control counters
- Data on opening/closing times of tracks at security checkpoints

4.5.4   In terms of real-time data exchange between the Queue Measurement System and ISH, the following technologies are supported and preferred:
- The Kafka protocol (client authentication and authorisation based on TLS)
- alternatively Kafka via REST API (client authentication and authorisation based on mTLS)
- JSON – transmission format encoded in UTF-8

4.5.5   The queue management system will also enable regular automated batch export of selected measured and stored data to the Prague Airport (EDW) data warehouse. The required data structure is specified in Annex 7 Data Storage Requirements. The general requirements for data transfer to the Prague Airport data warehouse are:

- A description of the data model is required, whether it is a relational model or a description of the columns in a csv file. The condition is the meaning of the individual columns, the designation of the keys (primary, foreign) and in what relation to other tables (files) it is. The delivered format can be a model in SAP PowerDesigner (16.0 and higher), Enterprise Architect (7.1 and higher) or a document in MS Office or Open Document. It must contain Data types, constraints, keys and bindings. Last but not least, business meaning and a description of individual attributes in entities (i.e. columns in tables).

- Data extract at least once a day. The options are in the form of an increment or a snapshot. Machine processing on the side of the data supplier is preferred to manual processing, which means errors and increased costs on the side of LPR.

- The form and method of transfer may be possible via File System, sftp/ftps, TCP/IP. For databases, active access by the data warehouse is required, i.e. the data warehouse downloads the data. For other forms (CSV, XML) it is up to agreement, the preferred option is the CAH ftps/sftp repository (ftp.cah.cz).

- The most preferred data interface is a connector directly to the database, namely to databases such as MS SQL or ORACLE. For less common databases, it is necessary to supply a Client for the MS Windows environment, ideally in both 64 and 32 bit versions. Furthermore, a description including the recommended settings for reliable data transfer functionality and information about the communication requirements of the given technology, i.e. TCP/UDP port.

- Another option is csv files, and for small data volumes also xml format in UTF-8 or CP1250 encoding. Files in .csv format will support enclosing text fields in quotes and a separator, ideally TAB, and standard Windows CRLF line breaks.

4.5.6   The Contractor must provide a data sample as part of the offer. The sample must contain data for at least 1 day related to a processor and a virtual boundary:
- for specific passengers: Passenger ID, queue arrival time, counter arrival time, counter departure time, process time, actual waiting time, predicted waiting time
- for specific passengers: Passenger ID, time of border crossing, direction of crossing
- for time intervals (ideally 1 min.): actual waiting time, predicted waiting time, queue length, throughput.

4.5.7   The System will be capable of sending text message notifications using the PrgAeroSmsService interface based on the REST API architecture running in Microsoft Azure. Client applications will be authenticated and authorised via the Azure Active Directory using OAuth 2.0 and JSON Web Tokens standards.

4.5.8   The system must be capable of sending e-mail notifications using the Exchange Web Service (EWS) API or its future more modern alternatives (Graph API).

Min. technické
podmínky_Min. tech

Data storage requirements

Passenger data

ID PAX	Queue entry time	Queue	Predicted waiting time [min]	Counter / track	Time of arrival at the counter	Time of departure from the counter	Actual waiting time [min]	Process time
monitored	monitored	monitored	calculated		monitored	monitored	calculated	calculated
101123	20.8.2023 10:23:10	T1_HRK_D_NONEU	7	T1_HRK_D_NONEU_6	20.8.2023 10:30:10	20.8.2023 10:30:50	8.2	0:00:40
101124	20.8.2023 10:35:17	T1_HRK_D_EGG	15	T1_HRK_D_EGG_6	20.8.2023 10:50:17	20.8.2023 10:51:17	16.1	0:01:00
102021	16.9.2023 9:35:15	T2_BEK_D_ECO	19	T2_BEK_D_ECO_6	16.9.2023 9:54:15	16.9.2023 9:56:15	22.4	0:02:00

Predicted and actual waiting time data – records for each minute and queue

Actual departure time	Predicted waiting time [min]	Actual waiting time [min]	Queue
20.8.2023 10:23:00	10	11	T1_HRK_D_NONEU
20.8.2023 10:23:00	1	2	T1_HRK_D_EGG
20.8.2023 10:23:00	6	8	T2_BEK_D_ECO
20.8.2023 10:24:00	9	10	T1_HRK_D_NONEU
20.8.2023 10:24:00	0	0	T1_HRK_D_EGG
20.8.2023 10:24:00	4	6	T2_BEK_D_ECO
20.8.2023 10:24:00	0	0	T1_HRK_D_EU

- **Locations to Be Monitored:**